



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**TECHNICAL AND OPERATIONAL ANALYSIS OF THE
FORTRESS SECURE WIRELESS ACCESS BRIDGE (ES-
520) IN SUPPORT OF TACTICAL MILITARY COALITION
OPERATIONS**

by

Sandy Geathers III

March 2008

Thesis Advisor:
Second Reader:

Edward L. Fisher
James F. Ehlert

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2008	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Technical and Operational Analysis of the Fortress Secure Wireless Access Bridge (ES-520) in Support of Tactical Military Coalition Operations			5. FUNDING NUMBERS	
6. AUTHOR(S) Sandy Geathers III				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) <p>Most networks, including those deployed in the Cooperative Operations and Applied Science & Technology Studies (COASTS) field experimentation program, utilize an access point, wireless bridge, switch, and security gateway. Reducing equipment requirements in the field is most desirable to minimize the equipment footprint, cost, and power required. The COASTS research group, involved in developing a scalable, multi-mission, system of systems for coalition environments, relies heavily on Commercial-Off-The-Shelf (COTS) network technology. Evaluating the performance of COTS technology such as the Fortress Secure Wireless Access Bridge (ES-520) directly supports the programs objectives.</p> <p>This thesis will analyze the performance of the Fortress Secure Wireless Access Bridge (ES-520) vs. traditional 802.11a/b/g wireless access points. Additionally, radio frequency (RF) propagation performance will be analyzed for distance, mobility, sustainability, and technical advantages/disadvantages with respect to varying antenna configurations and physical parameters such as climate and terrain. Testing and evaluation will be accomplished under the COASTS field experimentation program.</p>				
14. SUBJECT TERMS COASTS, C4ISR, IEEE 802.11 Technology, Wi-Fi, Wireless Networks			15. NUMBER OF PAGES 120	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**TECHNICAL AND OPERATIONAL ANALYSIS OF THE FORTRESS SECURE
WIRELESS ACCESS BRIDGE (ES-520) IN SUPPORT OF TACTICAL
MILITARY COALITION OPERATIONS**

Sandy Geathers III
Lieutenant, United States Navy
B.S., Southern Illinois University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

**NAVAL POSTGRADUATE SCHOOL
March 2008**

Author: Sandy Geathers, III

Approved by: Edward L. Fisher
Thesis Advisor

James F. Ehlert
Second Reader

Daniel C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Most networks, including those deployed in the Cooperative Operations and Applied Science & Technology Studies (COASTS) field experimentation program, utilize an access point, wireless bridge, switch, and security gateway. Reducing equipment requirements in the field is most desirable to minimize the equipment footprint, cost, and power required. The COASTS research group, involved in developing a scalable, multi-mission, system of systems for coalition environments, relies heavily on Commercial-Off-The-Shelf (COTS) network technology. Evaluating the performance of COTS technology such as the Fortress Secure Wireless Access Bridge (ES-520) directly supports the programs objectives.

This thesis will analyze the performance of the Fortress Secure Wireless Access Bridge (ES-520) vs. traditional 802.11a/b/g wireless access points. Additionally, radio frequency (RF) propagation performance will be analyzed for distance, mobility, sustainability, and technical advantages/disadvantages with respect to varying antenna configurations and physical parameters such as climate and terrain. Testing and evaluation will be accomplished under the COASTS field experimentation program.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PURPOSE OF RESEARCH	1
B.	RESEARCH QUESTIONS.....	1
C.	METHODOLOGY	2
D.	THESIS ORGANIZATION.....	3
II.	BACKGROUND OF FORTRESS TECHNOLOGIES AND COASTS	
	RESEARCH EFFORTS.....	5
A.	BACKGROUND	5
B.	COASTS 2007.....	6
1.	COASTS Overview	7
C.	INTRODUCING FORTRESS TECHNOLOGIES	9
1.	Fortress Technologies	9
D.	SECURE WIRELESS ACCESS BRIDGE (ES-520).....	10
1.	Radio Technology.....	11
2.	Mesh Architecture	12
3.	Security	14
4.	Hardware – Physical Attributes	16
5.	Configuration	17
E.	SUMMARY	18
III.	REVIEW OF RELATED THESES	19
A.	BACKGROUND	19
B.	WIRELESS COMMUNICATIONS NETWORK CONCEPTS	20
1.	Mobility.....	20
2.	Network Size.....	21
3.	Quality of Service.....	22
4.	Security	23
5.	Robustness	24
6.	Network Location.....	25
7.	Ad Hoc Architecture.....	26
8.	Routing Protocols.....	27
C.	SUMMARY	28
IV.	FORTRESS SECURE WIRELESS ACCESS BRIDGE (ES-520)	
	PERFORMANCE AND ANALYSIS	29
A.	INTRODUCTION.....	29
B.	AN OVERVIEW OF THROUGHPUT AND COVERAGE FACTORS..	29
1.	802.11 Protocol	29
2.	The Radio Environment	31
3.	Frequency	32
4.	The Vendor Equipment Design	33
5.	Vendor Interoperability	33

6.	Security	34
C.	MEASURING THROUGHPUT AND COVERAGE	34
D.	ES-520 NETWORK SUPPORTING HARDWARE AND SOFTWARE.....	35
E.	MEASURES OF EFFECTIVENESS AND PERFORMANCE.....	36
1.	Selected MOE and MOP	36
a.	802.11 Network - ES-520 MOE.....	36
b.	802.11 Network - ES-520 MOP.....	37
2.	Controllable Factors	39
F.	FIELD EXPERIMENTS	40
1.	Basis.....	40
2.	ES-520 Network Operating Areas.....	41
3.	ES-520 Network Configuration	43
4.	ES-520 Equipment Configuration	47
G.	RESULTS	47
1.	Run Options.....	47
2.	Test Setup	48
a.	Camp Roberts (CR).....	48
b.	Fort Hunter Liggett (FHL).....	49
3.	ES-520 Measures of Performance	50
a.	Camp Roberts	50
b.	Fort Hunter Liggett.....	51
H.	ANALYSIS	53
I.	SUMMARY	54
V.	FEASIBILITY, SUSTAINABILITY, AND TECHNICAL ADVANTAGES/DISADVANTAGES OF THE FORTRESS SECURE WIRELESS ACCESS BRIDGE (ES-520)	55
A.	BACKGROUND	55
B.	FEASIBILITY OF THE ES-520	55
C.	SUSTAINABILITY OF THE ES-520	59
D.	ADVANTAGES AND DISADVANTAGES OF THE ES-520	60
1.	Advantages.....	61
2.	Disadvantages.....	62
E.	SUMMARY	66
VI.	CONCLUSION	67
A.	RESEARCH SUMMARY	67
B.	OBSERVATIONS.....	67
C.	LESSONS LEARNED.....	69
D.	AVENUES FOR FUTURE RESEARCH	70
	APPENDIX: ES-520 NETWORK SUPPORTING HARDWARE AND SOFTWARE SPECIFICATIONS.....	71
	LIST OF REFERENCES.....	93
	INITIAL DISTRIBUTION LIST	97

LIST OF FIGURES

Figure 1.	Selected ES-520 MOE	37
Figure 2.	Selected ES-520 MOP	39
Figure 3.	CR Operating Area	41
Figure 4.	FHL Client Test Operating Area.....	42
Figure 5.	FHL Operating Area	42
Figure 6.	IxChariot Laptop and Root Endpoint Laptop used for ES-520 Network Testing.....	44
Figure 7.	Non-root Endpoint Laptop used for ES-520 Network Testing.....	45
Figure 8.	Non-root ES-520 Setup.....	46
Figure 9.	Basic ES-520 Network Diagram.....	46
Figure 10.	The Determinants of COTS Component Feasibility: Technical, Economic, and Strategic Constraints. (From: [15].)	57
Figure 11.	Fortress Technologies Secure Wireless Access Bridge (ES-520) (From: [18].).....	71
Figure 12.	Universal AC-to48V DC Power Adapter and AC Power Cord.....	74
Figure 13.	EBU-101-01 PoE Adapter (From: [19].)	75
Figure 14.	RJ-45-to-DB9 Adapter.....	1
Figure 15.	ES-520 Weatherizing Kit.....	1
Figure 16.	ES-520 Mast-Mounting Kit	1
Figure 17.	ES-520 Port Locations (From: [18].)	1
Figure 18.	RJ-45 and D89 Pin Numbering (From: [18].).....	78
Figure 19.	Weatherizing the RJ-45 Connector Boot Assembly (From: [18].).....	1
Figure 20.	Attaching the Front-Panel Cover (From: [18].)	1
Figure 21.	Attaching the Mast-Mounting Bracket and Grounding Stud (From: [18].).....	80
Figure 22.	Photo of 3COM Baseline Switch 2824-SFP Plus.....	1
Figure 23.	Photo of Marine Gel Battery.....	1
Figure 24.	PowerBright 1100 Watt 12 Volt DC-to-AC Power Inverter (From: [22].)	1
Figure 25.	Garmin Foretrex 201 (From: [23].).....	83
Figure 26.	Screen Capture of Google Earth Application	1
Figure 27.	Photo of Pacific Wireless 2.4 GHZ 7dBi Antenna (From: [24].)	1
Figure 28.	Photo of 5.8GHz 8dBi Superpass Antenna (From: Ref. [25].).....	1
Figure 29.	Photo of Hyperlink 5.8GHz 8dBi Antenna (From: [26].).....	1
Figure 30.	Photo of TerraWave 5.8GHz 10dBi Antenna (From: Ref. [27].)	1
Figure 31.	Photo of Hyperlink 5.8GHz 12dBi Antenna (From: [28].).....	89
Figure 32.	Screen Capture IxChariot Console.....	1

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Maximum Theoretical Performance for Various 802.11 Systems (From: [13].).....	30
Table 2.	ES-520 Network IP Addresses, Sub Masks, and Gateways	44
Table 3.	Component MAC Addresses	47
Table 4.	Run Options	48
Table 5.	Camp Roberts Distance Between Nodes and Elevation Difference	49
Table 6.	Fort Hunter Liggett Distance Between Nodes and Elevation Difference	50
Table 7.	Camp Roberts Throughput, Transaction Rate, and Response Time Results ...	50
Table 8.	Fort Hunter Liggett Throughput, Transaction Rate, and Response Time Results	52
Table 9.	Advantages of COTS Communications Technologies (From: [17].)	62
Table 10.	Disadvantages of COTS Communications Technologies in Military Applications (From: [17].)	65
Table 11.	ES-520 Specifications (From: [18].)	73
Table 12.	EBU-101-01 PoE Specifications (From: [19].)	77
Table 13.	EBU-101-01 PoE Pin Designators (From: [19].)	77
Table 14.	PowerBright 1100 Watt 12 Volt DC-to-AC Power Inverter Specifications (From: [22].)	83
Table 15.	Garmin Foretrex 201 Features (From: [23].)	84
Table 16.	Technical Specification of 2.4GHz 7dBi Pacific Wireless Antenna (From: [24].)	86
Table 17.	Technical Specifications of 5.8GHz 8dBi Superpass Antenna (After: [25].) ..	87
Table 18.	Technical Specifications of Hyperlink 5.8GHz 8dBi Antenna (After: [26].) ..	88
Table 19.	Technical Specifications of TerraWave 5.8GHz 10dBi Antenna (From: [27].)	89
Table 20.	Technical Specifications of Hyperlink 5.8GHz 12dBi Antenna (From: [28].)	90
Table 21.	Specifications of the Laptop Computers used in the Experimentation of the ES-520.....	92

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF SYMBOLS, ACRONYMS, AND/OR ABBREVIATIONS

2M	Miniature/Microminiature
AES	Advanced Encryption Standard
AP	Access Point
BER	Bit Error Rate
C2	Command and Control
C3	Command and Control Communications
C4ISR	Control, Communications Computers and Intelligence, Surveillance and Reconnaissance
CLI	Command Line Interface
cm	Centimeter
COASTS	Cooperative Operations and Applied Science & Technology Studies
COCOMO	Constructive Cost Model
COCOTS	Constructive COTS
COMLOG WESTPAC	Commander, Logistics Group Western Pacific
COMPACFLT	Commander, Pacific Fleet
COMSEVENTHFLT	Commander, Seventh Fleet
COTS	Commercial-off-the-Shelf
CR	Camp Roberts
CSMA/CD	Carrier Sense Multiple Access With Collision Detection
CTS	Clear-to-send
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DNS	Domain Name System
DoD	Department of Defense
EBO	Effects Based Operations
ES-520	Fortress Secure Wireless Access Bridge
FHL	Fort Hunter Liggett
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array

FSO	Free Space Optics
FTI	Future Technology Insertion
GHz	Gigahertz
GINA	Global Information Network Architecture
GUI	Graphical User Interface
HF	High Frequency
ICAO	International Civil Organization
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISR	Intelligence, Surveillance, and Reconnaissance
Km/h	Kilometers per hour
LAN	Local Area Network
LOS	Line-of-Sight
MAC	Media Access Control
MANET	Mobile Ad Hoc Networking
Mbps	Megabit per second
MCA	Multi-Channel Architecture
MIL-STD	Military Standard
MIMO	Multiple-input multiple-output
MIO	Maritime Interdiction Operation
MOE	Measures of Effectiveness
MOP	Measures of Performance
MSP	Mobile Security Protocol
MTBF	Mean Time Between Failure
NCW	Network-Centric Warfare
NEMA	National Electrical Manufacturers Association
NGO	Non-governmental Organization
NIST	National Institute of Standards and Technology
NPS	Naval Postgraduate School
NRL	Naval Research Laboratory
NTDR	Near Term Digital Radio

OFDM	Orthogonal Frequency-Division Multiplexing
ONR	Office of Naval Research
OSD	Office of the Secretary of Defense
PC	Personnel Computer
PCB	Printed Circuit Board
PCF	Point Coordinating Function
PDA	Personnel Digital Assistant
PHY	Physical
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PSE	Power Searching Equipment
QoS	Quality of Service
R&D	Research and Development
RF	Radio Frequency
rMSP	Routable Mobile Security Protocol
RTS	Request-to-send
S&T	Science and Technology
SA	Situational Awareness
SATCOM	Satellite Communications
SBU	Sensitive But Unclassified
SEACAT	Southeast Asia Cooperation against Terrorism
SLA	Service Level Agreement
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TOC	Tactical Operations Center
TRNG	True Random Number Generator
UAV	Unmanned Aerial Vehicles
UCSC	University of California, Santa Cruz
USB	Universal Serial Bus
USC-CSE	University of Southern California-Center for Systems and Software Engineering
USPACOM	United States Pacific Command

VDC	Volts Direct Current
VHF	Very High Frequency
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WINGS	Wireless Internet Gateway
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

ACKNOWLEDGMENTS

Primarily, I would like to thank my family, Karvette, Khalid, and Makhi, for their loving support during my stay at the Naval Postgraduate School and for their understanding; I needed time away from home to complete my research. I would also like to thank Mr. James Ehlert and Mr. Edward Fisher for allowing me to join COASTS and for their help in making my research come to completion. Additionally, Mr. Scott Howard of Fortress Technologies was instrumental in helping with the setup of all experiments. Without his help, I would have not been able to collect the data for this thesis.

Finally, I would like to express my most sincere gratitude to all COASTS participants. Each person of the team provided insight, technical expertise, and camaraderie during each phase of COASTS 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE OF RESEARCH

Wireless technology has changed, and is continuing to change, the way military and civilian organizations run day-to-day operations. As this technology evolves, wireless devices improve and combine technologies and capabilities to reduce equipment needed within a network or mesh. This reduction of equipment provides more affordability, increased mobility, ease of deployment, and increased flexibility.

With the introduction of Fortress Technologies Secure Wireless Access Bridge (ES-520), the Cooperative Operations and Applied Science & Technology Studies (COASTS) program was able to reduce required equipment and was able to provide better tactical scenarios for later experiments. Overall, the ES-520 could reduce requirements needed for tactical wireless networks while still maintaining maximum battlefield awareness.

B. RESEARCH QUESTIONS

Primary question: What are the network performance characteristics of the Fortress Secure Wireless Access Bridge (ES-520) using varied antenna configurations and physical conditions, such as climate and geography? Secondary questions include:

1. What is the network reliability of operating the ES-520 in different environments?
2. What are the advantages/disadvantages of the ES-520 as compared to other Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g network access points?
3. What is the optimum antenna configuration for network communications in terms of clients and as a network relay device?

4. What is the maximum range, associated signal strength, and how well does the optimized configuration perform in terms of throughput at various points in the network?
5. What is the minimum mounting height of the antenna that will provide acceptable performance?

C. METHODOLOGY

The methodology consisted of research of available literature, both hard copy and electronic, as well as testing and evaluation of the ES-520 network. The research methodology was conducted as follows:

1. Development of Metrics and Test Plan. This phase included the necessary academic review of existing technical material for the ES-520. Measure of Performance and Measures of Effectiveness (MOP/MOE) were created. These were used to develop an effective test and evaluation plan.
2. Conducted Field Experimentations. Perform field experiments recording results obtained in support of development of an IEEE 802.11 wireless tactical network to be deployed and operated in support of military field exercises.
3. Analysis of Results and Conclusions. The results were analyzed by previously determined MOP/MOE's. By comparing the results from MOP/MOE's, one can determine the effectiveness and feasibility of deploying the system in real-world military operations or environments.

D. THESIS ORGANIZATION

Chapter II provides a discussion of military requirements for secure wireless communications, the COASTS 2007 international field experimentation program, and the ES-520 capabilities.

Chapter III provides an overview of previous research that evaluated military necessity versus the current state-of-the-art in 802.11 devices.

Chapter IV discusses the methodology used in the research of the ES-520 as well as provides an analysis of the results with regard to the MOEs and MOPs to address the capabilities and limitations of the equipment.

Chapter V provides a review of the feasibility, sustainability, and technical advantages/disadvantages of the ES-520. Chapter VI recommends future implementation and experimentation in the COASTS environment as it pertains to high throughput tactical wireless networking regarding COTS 802.11 technology.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND OF FORTRESS TECHNOLOGIES AND COASTS RESEARCH EFFORTS

A. BACKGROUND

The world of military communications is on the verge of massive and revolutionary change, from new generations of satellites providing greatly enhanced bandwidth, speed, and capability to the final realization of a two-decade drive toward a networked battlefield. This change is greatly influenced by advances in wireless capabilities. Wireless technology has a large influence on tactical communications; therefore, the impact of growth in wireless communications will change the way the military operates in the tactical environment. Wireless data communications on the battlefield have been available only at very low transfer rates over high frequency (HF) or satellite communications (SATCOM). Reversing that is one of the major goals of short- and long-term systems in development. Although there is an increase for the use of wireless technology, some challenges arise in the culmination of the capability in the battlefield.

The most obvious challenge for the battlefield is sheer capacity. The military's appetite for wireless bandwidth is never satisfied, with sensors and data-acquiring devices competing with warfighter communications for airtime in an effort to provide decision makers the most complete operational picture and enable the network-centric warfare (NCW) concept. Interference is an even tougher challenge than bandwidth because tall towers--which in the commercial world provide line of sight over hilltops, trees, and buildings, are risky to erect on the battlefield. Communications jamming is another problem that most commercial users do not have to overcome. Emissions security is a concern, where any source of radio wave signals represents a potential target to the enemy--the more emissions, the more valuable the target. In order to overcome these obstacles, secure communication products and solutions are needed to connect and provide transmission, processing, recording, monitoring, and dissemination functions for a variety of communication systems, such as:

1. Secure data links to and from airborne, satellite and ground- and sea-based remote platforms for real-time information collection and dissemination to users
2. Highly specialized fleet management and support, including systems integration, sensor development, modifications and maintenance for signal-intelligence and special-mission aircraft, as well as airborne surveillance systems
3. Strategic and tactical signal intelligence systems that detect, collect, identify, analyze, and disseminate information
4. Secure telephone and network equipment and encryption management
5. Communication systems for surface and undersea vessels and manned space flights [1]

These are the areas where the military needs to focus its research efforts, preferably finding ways to adapt COTS products to meet these requirements. Achieving that goal will require evolutions in tactics, techniques, and procedures as well as equipment from the national command authority level down to the individual warfighter. Key to making this work on the battlefield will be creating a gateway functionality that will make the entire operation transparent to the users. One military program that tries to tackle these challenges is the Naval Postgraduate School's COASTS international field-testing and thesis research program.

B. COASTS 2007

Indonesia, Malaysia, Singapore, Thailand, and the United States are countries involved in COASTS Research and Development (R&D) to investigate COTS Command and Control, Communications Computers and Intelligence, Surveillance and Reconnaissance (C4ISR) technologies to provide real-time situational awareness (SA) for multi-national, tactical and remote decision makers in a cooperative environment. Annually in May and June, an experiment is conducted that spirally builds on the

successes of that from previous years. COASTS-07 is the third consecutive year for this series of field test experiments, and will build upon the lessons and successes from past years. Additionally, COASTS-07 plans to employ several select technologies into two major Pacific Fleet exercises. The two exercises are; TALISMAN SABER 2007 with Commander, Seventh Fleet (COMSEVENTHFLT) in Australia during June 2007 and Commander, Logistics Group Western Pacific (COMLOG WESTPAC's) Southeast Asia Cooperation against Terrorism (SEACAT) 2007 exercise in Singapore 14-22 August 2007 [2].

1. COASTS Overview

As stated in the previous section, the COASTS field experimentation program consists of U.S. and international partners. Within this organization are NPS faculty and students with support provided by Office of Naval Research (ONR) Reservists. Funding and requirements are provided by the Office of the Secretary of Defense (OSD) and the Department of Homeland Security (DHS) and their agencies. Another major sponsor is the Department of Defense (DoD) and DHS. Both commands and agencies provide COASTS operational guidance, and in some cases direct participation in the experiment. Commands and agencies from the participating countries provide support and are essential to the success of COASTS. Finally, commercial vendors are within the organizational group to provide COTS technologies and expertise to support the overall program objectives. Each part of COASTS organization integrates to create the deployed Global Information Network Architecture (GINA)/COASTS system [2].

The COASTS-07 mission engages these international and domestic partners at the R&D level through cooperative Science & Technology (S&T) field experimentation. Specific COASTS-07 objectives include:

1. Investigate net-centric information management and Effects Based Operations (EBO) in a multi-national environment across tactical, operational, and strategic domains
2. Make Intelligence, Surveillance, and Reconnaissance (ISR) data and information visible, available and usable when and where needed

3. Create synergy with the Theater Security Cooperation Plan and supporting theater objectives (long-term influence)
4. Expand the scope of maritime research into improved command and control (C2) technologies for Maritime Interdiction Operations (MIO)
5. Demonstrate ship-to-ship and ship-to-shore communication capabilities in deployable form factors
6. Investigate deployment issues surrounding hastily formed networks in rugged and varied terrain under adverse climatic conditions
7. Increase situational awareness for the disadvantaged (tactically-engaged) user, and improve the bi-directional flow of information between forward employed personnel and their tactical, operational, and strategic operations centers and headquarters
8. Identify, test, and evaluate biometric technologies, with the intent to conduct Identity Management in real time across a globally distributed network
9. Investigate the utility of mini-Unmanned Aerial Vehicles (UAVs) and sensor suites in rainforest, littoral, and maritime environments
10. Investigate integration issues surrounding non-governmental organization (NGO) and international partner participation
11. Investigate the dissemination, parsing, protection, security, and sharing of information between various U.S., international, and commercial partners
12. Partner with U.S. Pacific Command (USPACOM), Commander, Pacific Fleet (COMPACFLT) and COMSEVENTHFLT to integrate selected COASTS technologies into exercise TALISMAN SABER-07
13. Partner with Commander, Logistics Group Western Pacific (COMLOG WESTPAC) to integrate selected COASTS technologies into exercise SEACAT-07 [2]

C. INTRODUCING FORTRESS TECHNOLOGIES

Due to the requests to NPS from friendly nations, there is an immediate requirement for low-cost, state-of-the-art, real-time threat warning and tactical communication equipment that is rapidly scalable based on operational considerations. Currently, most tactical systems lack the capability to rapidly enable a common information environment amongst air, surface, and sub-surface entities via a self-forming, self-authenticating, autonomous network. Various COTS technologies exist that can satisfy some of these requirements. However, COTS technologies typically do not meet all of the DoD and friendly nation requirements associated with security missions. Hence, a central role of the COASTS field experimentation program is to demonstrate that NPS, in conjunction with friendly nation organizations and commercial vendors, can integrate COTS capabilities currently available into a larger system of systems to satisfy technical and tactical mission requirements [2]. One of the commercial vendors that provide COTS capabilities is Fortress Technologies.

1. Fortress Technologies

Fortress Technologies designs, develops and manufactures market leading wireless infrastructure and software solutions for secure mission critical communications. Rigorously tested and proven, Fortress products provide government and commercial customers secure wireless capabilities across fixed, portable, and mobile environments – from the tactical edge to municipal networks. Fortress’ flexible and resilient solutions enable immediate “on demand” secure voice, video and data communications virtually anywhere and across all wireless transports - including Wireless Fidelity (Wi-Fi) (802.11), Worldwide Interoperability for Microwave Access (WiMAX) (802.16), Free Space Optics (FSO), Military Radio Frequency (RF) and satellite [3].

Fortress designed wireless infrastructure and software solutions from the ground up to create a highly integrated and versatile wireless communications platform that government customers could rely on in fixed, portable or mobile environments. The design centered on customers’ needs for Maximum RF Range, Broadband Performance,

Network Resilience and High Assurance Security in an integrated end-to-end solution that could be rapidly deployed in harsh environments across dynamic network topologies.

Supporting the operational requirements in these environments required applying a new approach to wireless network technologies, design, and architectures. Supporting military units in the field is challenging. Fortress' approach integrates numerous technologies and capabilities into a single communication platform built on a secure peer-to-peer architecture. Fortress utilizes its Macromesh technology to create highly dynamic and robust networks with self-forming, self-healing, path-optimizing capabilities that can support thousands of wireless mesh nodes in a highly mobile network. To accomplish this, Macromesh incorporates both proactive and reactive routing algorithms into a Layer 2 meshing protocol that requires less than 5% of the bandwidth for control traffic regardless of the network size. Furthermore, Fortress has implemented Federal Information Processing Standard (FIPS) certified Layer 2 Advanced Encryption Standard (AES) encryption to protect both the data in transit and the network itself, complying with the various government wireless and security policies. Fortress has implemented these technologies into both wireless infrastructures, such as the ES-520 and client software products [3].

D. SECURE WIRELESS ACCESS BRIDGE (ES-520)

The Fortress ES-520 enables organizations to establish a high-performance wireless mesh network by combining the functions of an access point, switch, wireless bridge, and security gateway in a form factor engineered specifically for harsh outdoor environments. The ES-520 weighs less than 5 lbs and uses less than 12 watts of power while providing superior performance in distance and throughput. Coupled with industry leading client support, Fortress offers an end-to-end solution that supports robust communications from the vehicle to the warfighter or first responder under high tempo mobility.

The ES-520 enables organizations to rapidly establish a high-performance wireless mesh network by combining the functions of an access point, switch, wireless

bridge, and security gateway in a form factor engineered specifically for harsh outdoor environments. There are five main attributes to the ES-520:

1. Radio Technology
2. Meshing Architecture
3. Security Capabilities
4. Physical Attributes
5. Flexible Configuration [3]

These attributes in the ES-520, along with the broad client support, work seamlessly to create an end-to-end solution that supports challenging deployment environments. The upcoming sections describe the design methodology used to implement the five design attributes outlined above. Some of the features described in these sections are planned features, and some features are optional in the operation of the product.

1. Radio Technology

Radio performance is perhaps the most visible attribute of the ES-520. The ES-520 line-of-sight (LOS) performance using Omni-directional antennas allows use of the product in true mesh and ad-hoc configurations without reliance on directional antennas, which limit such configurations. The radio technology design methodology of the ES-520:

1. Provides the highest throughput and range by utilizing the best radios available, combined with a high quality Printed Circuit Board (PCB) design to reduce noise, which provides industry leading radio performance. Not only does the low level optimization done at the Media Access Control (MAC) and Physical (PHY) level result in greater radio sensitivity, the ES-520 is very light and pole-mountable to decrease signal loss through cables.

2. Uses standard socket interfaces to allow for best of breed COTS, semi-custom and full custom radio design. This flexibility allows the ES-520 to keep up with the rapidly changing radio technologies and support customer-specific configurations of radios.
3. Aggressively follows radio technology using standard and custom radio designs. This radio technology roadmap includes 802.11n Multiple-input multiple-output (MIMO), 4.9GHz WI-FI, etc [3].

2. Mesh Architecture

The ES-520 supports two mesh technologies, Micromesh and Macromesh. Micromesh is included as a primary feature in the base ES-520. Micromesh provides the self-forming and self-healing capabilities core to any mesh architecture. Micromesh is designed to support fixed infrastructure or portable networks where the infrastructure is relatively static. Macromesh, on the other hand, is designed to support large, dynamic networks with more emphasis on mobility and scalability. Macromesh offers significant advantages over Micromesh in terms of scalability and resiliency, which is particularly important in highly mobile environments. Macromesh is also implemented in the Fortress software client, providing the ability to utilize not only network infrastructure devices but also user input devices such as laptops, tablets and handheld Personnel Digital Assistants (PDAs) to forward data and operate as part of the mesh network. These input devices can use Macromesh to form their own ad-hoc mesh networks as well. Fortress Macromesh possesses attributes of scalability, mobility, low overhead and dynamic self-configuration, and self-administration that are unique. Macromesh supports:

1. Large scale networks (thousands of nodes)
2. Highly mobile networks - including 'fast mover' nodes
3. Extremely low bandwidth networks
4. Networks spanning vehicles, aircraft and fixed wired installations

5. Regardless of network size, less than 5% of bandwidth is needed for control traffic
6. PC-based mobile ad-hoc networking [3]

All current self-forming, self-healing networks are extremely limited in size and their ability to organize mobile networks. This fundamental problem exists because the amount of control bandwidth required to keep the network ‘whole’ grows at an exponential rate with network size. This means that by the time even a small mesh network is deployed it requires all of the available bandwidth just to maintain itself. Fortress Macromesh overcomes this serious problem. Regardless of network size or network bandwidth, Fortress Macromesh will incorporate both proactive and reactive routing algorithms into a Layer 2 meshing protocol that requires less than 5% of available bandwidth.

Macromesh features are well suited for highly mobile tactical edge environments because of the following attributes:

1. Scalability – Macromesh is designed to support thousands of nodes and an equally large network diameter. Macromesh is designed from the ground up for large mesh networks and incorporates both proactive and reactive routing algorithms. Proactive algorithms are necessary to sustain a high level of mobility, while reactive protocols are utilized to support very large networks.
2. Enhanced network mobility – Macromesh supports automatic configuration of Internet Protocol (IP) addresses and distribution of node names without reliance on any centralized server such as Domain Name System (DNS) or Dynamic Host Configuration Protocol (DHCP). This is critical to supporting a large resilient mobile network.
3. Administrative Flexibility – Macromesh provides significant enhancements to support highly efficient multicast mechanisms. In

addition, network segregation allows the network operator to segment the network into multiple administrative domains to put better control mechanisms in place [3]

3. Security

The ES-520 builds upon Fortress' extensive experience in providing high assurance security products to the government for over a decade. The ES-520 and Fortress Secure Clients incorporate multi-layer and multi-level security architecture critical to ensure the protection of the network and communications. The Fortress security foundation is built on a Layer 2 peer-to-peer architecture, which adheres to the Federal Government's stringent security policies. Another compelling aspect of Fortress Security is that as a Layer 2 protocol, it supports and works across Layer 2 mesh architectures.

The ES-520 utilizes multiple layers of security. Below the layers are listed:

1. Encryption

- a. National Institute of Standards and Technology (NIST) FIPS 140-2 AES 128, 192 & 256
- b. IEEE Wi-Fi Protected Access 2 (WPA2) (802.11i)
- c. Fortress media independent layer-2 Mobile Security Protocol (MSP)
- d. Fortress media independent layer-3 Routable Mobile Security Protocol
- e. (rMSP) which is available as a value-add module
- f. Suite B implementation is available as a value-added module

2. Multi-factor Authentication

- a. Network, Device, User including DoD Common Access Cards or tokens

- b. Internal or external authentication server including: RADIUS, DoD Public Key Infrastructure (PKI)
- 3. Wireless Intrusion Detection Module
- 4. Rugged, tamper-evident enclosure [3]

The ES-520 also utilizes multiple levels of security. Below the levels are listed:

- 1. Commercial
 - a. Highest level COTS product available
- 2. Government
 - a. Sensitive But Unclassified (SBU) – NIST FIPS validation
 - b. Classified – Suite B module available [3]

All these security standards are built and evaluated against the rigorous FIPS 140-2 Level 2 and Common Criteria Level 3 Wireless Local Area Network (WLAN) Protection Profile. The ES-520 utilizes advanced security functions, which are implemented in a reconfigurable, field upgradeable custom field programmable gate array (FPGA). This particular implementation, which is unique to the ES-520, provides a number of significant advantages including:

- 1. Fast crypto (40 Megabit per second(Mbps)): highest performance in it class
- 2. Protection against timing attacks: where the timing of cryptographic operations is data-dependent. The AES key has been shown to be vulnerable to timing attacks using a simple Cache Timing attack.
- 3. True Random Number Generator (TRNG): The cornerstone of good cryptography is the reliance on random numbers. Appliances such as an ES-520 have no way to gather entropy because there is no direct user interaction with the device (such as mouse moves and keyboard

input). Thus, for a truly secure implementation, the ES-520 includes True Random Number Generators. This feature is unique to the ES-520.

4. Upgradeability: The ES-520 platform built on FPGA technology allows the security subsystem to support emerging security standards with in-field upgrades without compromising the strength of the implementation.
5. Hardware compression: The ES-520 implements hardware compression before encryption. In addition to the added security benefits, it helps preserve valuable wireless bandwidth. Depending on the data mix, up to a 400% increase in throughput is possible [3]

4. Hardware – Physical Attributes

The ES-520 is designed as highly integrated, flexible, lightweight, and rugged platforms designed for harsh environments and include the following attributes:

Dual radios (support for a third radio)

1. 8 – Local Area Network (LAN) ports, 1 – Wide Area Network (WAN) port, Universal Serial Bus (USB) port and dual serial port (one for management and the other for connection to a serial device, e.g., satellite)
2. Integrated lightning arrestors, a grounding strap, and variable voltage input of 9 Volts Direct Current (VDC)-36VDC and 48VDC
3. Maximum power draw of 13 Watts
4. The ES-520 can be powered by Power over Ethernet (PoE) and power other devices using PoE Power Searching Equipment (PSE) mode over the 8 - LAN ports
5. Lightweight (5lbs) and highly compact (8.8” x 2.66” x 8.22”) form factor

6. National Electrical Manufacturers Association (NEMA)-4 and Military Standard (MIL-STD) 810F certification
7. Custom design of PCB and enclosure provides higher resilience to power glitches while isolating the radio from unclean power sources [3]

5. Configuration

The ES-520 was designed to support rapid deployment hence significant emphasis and effort was placed on simplifying and automating the configuration:

1. The ES-520 utilizes a single user interface to configure a multitude of functions (security, radios, authentication, etc.). This greatly reduces the learning curve for the product.
2. The ES-520 securely propagates the configuration from one node to other nodes over both the wired and the wireless interfaces. The operator is able to take new ES-520 (slave) units and have these units receive their configuration securely from other nodes (master) in the network without the need to use a Command Line Interface (CLI) or Graphical User Interface (GUI) on the slave units. Simultaneous configuration of multiple slave units is also supported.
3. Using the external recessed keys the ES-520 can be zeroed to bring it back to a factory-fresh configuration. This affords the operator the flexibility to zero the keys for security reasons, or repurpose a box for a different application with little effort.
4. In a future software release, the ES-520 will support the ability to receive its configuration from a USB flash disk. The configuration will be encrypted on the flash disk. The operator will be able to transfer the configuration from the USB disk to the ES-520 with a set of predetermined key sequence using the recessed switches on the front

panel. This will allow the operator to separate the place where the configuration is created and where the configuration is physically applied to the device [3]

E. SUMMARY

This chapter discussed the COASTS 2007 international field experimentation program and Fortress Technologies Secure Wireless Access Bridge. The next chapter will discuss previous related theses with relevance to the two radios in the ES-520 in context with military shortfalls.

III. REVIEW OF RELATED THESES

A. BACKGROUND

NCW is mostly associated with wireless networks. The military is interested in NCW because they must protect mobile military networks from intrusions and attacks. Increasingly, military operations require wireless network connectivity for the flow of command and control information from the central command to the deployed field units. Since the military is a highly mobile entity, it requires networks that can be set up and configured in an ad hoc fashion. Moreover, since security and mobility are critical factors to the military, securing mobile ad hoc networks is an area worthy of focus [4].

Wireless technology is an integral part of COASTS field experiments. COASTS field experiments include scenario narratives that describe situations within which the military may need to operate. Military personnel, including military network operators, use these experiments to predict outcomes for future operations. The experiments also provide military network designers with a context in which to identify specific products that meet the requirements of the specific situation. This context is especially important for wireless network designers, who must build military mobile ad hoc networks that are interoperable, manageable, and secure.

Network architectures for operational experiments must be evaluated against design criteria to ensure they are suitable for the mission or the purpose for which they are designed. This is especially important for military operations that are derived around network architectures based on existing and emerging COTS products, services, and standards. Suitability of commercial products, services, and standards must be evaluated for military purposes. The evaluation criteria are the concepts that form the basis on which the architecture was designed. The outcome is a set of concepts with which one can design and evaluate the make-up of architecture for an operation. In turn, modifications of the concepts result in fine-tuning a suitable architecture for the operation.

Military operations and experiments should consider wireless networking concepts, such as mobility, network size, and quality of service (QoS), among others, as important factors when designing military ad hoc network information operations. The next section reviews several of these concepts in context of military necessity versus the current state of the art in 802.11 technologies.

B. WIRELESS COMMUNICATIONS NETWORK CONCEPTS

Wireless communications networking concepts, such as mobility, network size, and QoS are integral factors in limiting the scope of a networking demonstration for a particular scenario. The concepts form the assumptions for network design, and the connection integrity in a network depends on these concepts and their respective parameters. Military scenarios that involve wireless networks provide for environments that stretch the integrity of network connectivity. Thus, before the scenario exercise, these networking concepts must be analyzed and evaluated during the scenario design phase. Mobility, network size, and QoS are a few of these concepts. A secure mobile ad hoc network must also be designed to be robust, have adaptive routing, and manage mobility with control protocols [4]. These concepts and their corresponding relation to an applied military scenario are explained in further detail in this section.

1. Mobility

Mobility is a necessity in military operations. While moving, the forces require connectivity for voice, data, and perhaps video. Therefore, mobility is a basic assumption in military network design. The network should be autonomous, capable of self-forming, and self-maintaining so that it can be deployed anywhere without the need for infrastructure. Thus, the network itself should be mobile and “ad hoc.” The nodes within a military network are also mobile. These nodes consist of soldiers with PDAs, armored vehicles, tanks, UAVs, and manned aircraft.

An important parameter to consider for mobility is speed. Doppler effects, fading, and shadowing are among the impairments of the received signal that are directly related to mobility and the speed of a node. A wireless receiver in a mobile ad hoc network

should be designed to adapt to the changes in conditions of the radio channel being used. Nodes may be stationary sensors, as slow as soldiers on foot, or as fast as ground vehicles, helicopters, UAVs, or jet aircraft.

In [5], the purpose was to study experimentally the behavior of an IEEE 802.11 wireless network when the nodes are characterized by mobility up to the speed of 240 kilometers per hour (km/h). This study leads to the understanding of the survivability and the performance of a connection under various aggressive mobility conditions. These studies may be adapted for data telemetry from mobile airborne nodes to fixed networks or between airborne nodes.

2. Network Size

Network size may be determined as a measure of the number of nodes in a network, the coverage (range) of the network, or both. Range is defined as the radius of Omni-directional coverage, or the maximum distance that the signal may travel in one dimension with reasonable reception. Although often used interchangeably, range and coverage are not the same. Directional antennas provide poor coverage with very short range in all directions except for those designated by design. Reasonable reception means sufficient signal strength for the receiver to obtain an acceptable error rate. Both range and coverage are specified as averaged measurements of sufficient signal strength in different environments and terrains [4].

A large number of nodes may be densely populated in a command center, or may be sparsely distributed in the mountains. In both cases, the size of the network is an important design consideration. It affects the integrity of network connectivity not only through capacity impairments due to high traffic, but also through range effects on signal strength. If the network is too densely populated with active nodes, the generated traffic limits network availability by exceeding the network's capacity. If the network is too sparse, parts of the network may be left without radio coverage due to insufficient signal

strength. Thus, it is important to look at network size, and its parameters, range and capacity, as a concept whose analysis provides much input to designing a network for a military operation.

In [6], the research discusses consideration of ad hoc network selection. When considering network size users must consider how to configure the ad hoc network. The configuration of an ad-hoc network can be either hierarchical or flat. In a hierarchical network, the network nodes are partitioned into groups called clusters. Within each cluster, one node is chosen to perform the function of a cluster head. Routing traffic between two nodes that are in two different clusters is always through the cluster heads of the source and destination clusters. In a flat ad-hoc network, all nodes are equal. Connections are established between nodes that are in close enough proximity to allow sufficient radio propagation conditions to establish connectivity. Routing between any two nodes is constrained only by the connectivity conditions and, possibly, by security limitations. Additionally, the research demonstrates that the flat network architecture is should be chosen in military-type of ad-hoc networks, due to its high resilience to failures.

3. Quality of Service

Networks are not just about connectivity. The QoS provided by a network is important and can be measured using several parameters. QoS parameters for wireless networks include delay, capacity, range, and the bit error rate (BER). It is essential that a service provided through the wireless medium has a low latency and arrives reliably at its destination. The tolerances for each of the QoS parameters needed to assure the quality of the service vary depending on the application. The majority of the delay comes from the wireless device's processing power and available bandwidth. Propagation delay in this application tends to be minimal because radio waves travel at the speed of light. Capacity poses a problem when too many users are competing for limited resources or high bandwidth applications are utilized on low-bandwidth connections. Range becomes important when the wireless user reaches the edge of the radius of coverage. Generally, delay is measured in seconds, capacity in bits per second, and range/coverage in meters.

The BER is a measure of noise or interference in the communications channel. Just like range, capacity, delay, and BER, security should also be considered a measurement of QoS [4].

In [7], the study suggests a node-centric solution, based on priority queues at the node, for providing QoS guarantees. Additionally, the study proposes another scheme wherein the access points, the elements that control the Point Coordinating Function (PCF) part of channel access, will communicate and coordinate amongst themselves to provide better service and avoid the total denial of service to mobile nodes. By theoretical analysis and simulation results, it shows that the extensions proposed will enhance the throughput and help in giving better QoS guarantees in the 802.11 domain.

4. Security

Network security is characterized by the following attributes as authentication, non-repudiation, confidentiality, data integrity, and availability. Integrity may be measured in terms of errors that are introduced into the data. Error correction and error checking methods can also highlight if the data has been tampered with or spoofed. Availability is often measured in units of time. Mean Time Between Failure (MTBF) of a network is a statistical indication of how long the network was disconnected and inaccessible to the users.

Unfortunately, unlike integrity and availability, there are no clear, standardized ways to measure the other security attributes: authentication, non-repudiation, and confidentiality. Scientifically, the methods and algorithms applied to these concepts are only as good as the last person who attempted to break them. For example, confidentiality can be mitigated with encryption. The quality of cryptographic algorithms is statistically measured as a function of the time; how long would it take someone to break them.

Authentication is the verification of the identity of users in a communication network. It is a key network security concept because it is the first step towards the prevention of unauthorized access to network resources and sensitive information. As opposed to commercial networks where authentication is secondary to system discovery

and routing, this concept is primary to military environments. As an added layer of protection, mutual authentication verifies the network to the user as well as the user to the network. This guards against a user giving his or her credentials to network that only appears legitimate. Authentication requires key management for the secure creation and distribution of the cipher keys that allow the users access to the network.

Non-repudiation provides proof that a particular user performed a particular action at a particular time. It is used to record the origin and date of information so that the communicated facts cannot be disputed later. Non-repudiation is essential in military environments where national security is at stake. Moreover, the enabling technologies for this concept may be used as proof in courts for judicial law enforcement.

Given the nature of military information in a coalition environment, data should be transferred within common security architecture to allow secure, seamless communication across different wired and wireless network technologies, devices, and applications. COTS products can make this commonality possible so that the networks of different coalition partners can interoperate with one another.

To demonstrate the importance of security, [8] provides an experimental analysis 802.11-specific attacks. In addition, it provides a description of vulnerabilities in the 802.11 management and media access services that are vulnerable to attack. Then the research exhibits that all such attacks are practical to implement by circumventing the normal operation of the firmware in commodity 802.11 devices. Additionally, it implements two important classes of denial-of service attacks and investigates the range of their practical effectiveness. Finally, it describes, implements, and evaluates non-cryptographic countermeasures that can be implemented in the firmware of existing MAC hardware.

5. Robustness

A military wireless network should provide sufficient connectivity under harsh conditions for command and control communications (C3) services. Network nodes may be destroyed or compromised by the enemy. Jamming techniques may reduce

connectivity and hinder QoS. A distributed network topology, as opposed to a centralized one, increases the availability of the network by reducing the probability of having one point of failure for the entire network. Distributed ad hoc networks, on the other hand, are difficult to manage. Routing and security implications such as key management are quite challenging in these networks.

A network should also be able to adapt its QoS to the demands of the military scenario. Commercial networks are designed to track the harsh conditions of the wireless medium and to provide a steady predictable QoS over time. However, it is crucial for a military network to adapt to the demands of the situation. Functions such as point-to-point, multicast, and broadcast are critical to military scenarios and must remain operational. The integrity of the connection with these functions may come at a cost to QoS. A military network should be able to compromise certain attributes in favor of others in order to maintain the integrity of the connection. For example, it is common in short-lived ad hoc networks under severe conditions to sacrifice certain security attributes in order to gain the benefit of higher bandwidth and lower delay.

In [9], the research provides a discussion about robustness to jamming, denial of service, and spoofing attempts, and robustness to random node failures (either due to adverse propagation conditions or to radio failures). This discussion compares the following existing wireless radio systems; the Near Term Digital Radio (NTDR), VRC-99, IEEE 802.11, International Civil Aviation Organization (ICAO) Very High Frequency (VHF) Data Link Mode 3, Naval Research Laboratory (NRL) Multi-Channel Architecture (MCA), University of California, Santa Cruz (UCSC)/Rooftop Communication Wireless Internet Gateway (WINGS), and Mobile Ad Hoc Networking (MANET).

6. Network Location

A secure mobile ad hoc network may be placed on either hostile or friendly ground to provide connectivity for strategic, operational, or tactical purposes. It may be on dry land or a maritime environment. On dry land, building density may be classified

as downtown, urban, or suburban on terrain that can be either flat or mountainous. In maritime environments, the sea conditions and the weather should be taken into considerations for network design. These concepts directly affect the wireless channel conditions.

It is interesting that security risk is described as a function of the external parameters to the network (threats), internal parameters of the network (vulnerability), and the potential aftermath of the damage to the network (impact). The deployed location of a wireless network directly affects its internal and external vulnerabilities and threats. Network architects should consider these in their design and assess the potential risks to the network.

In [10], the research uses AVAYA WP-II E model by Lucent Technologies to propose a method based on neural networks for reducing the errors in the determination of the current location of the user. The research collects measurements of the strength of signals coming from the different antennas at a series of points distributed in the environment. These data are a training set that can be used by a learning algorithm (neural net) to develop an association between signal strengths and location. Based on the collected data, it proposes the use of neural networks and a training algorithm based on second order information in order to develop flexible models of the relationship between the raw signal measurements and the location data.

7. Ad Hoc Architecture

A military wireless network should have a distributed topology. Non-centralized architectures eliminate single points of failure. The network should also be self-organizing and dynamically hierarchical in order to function autonomously with little or no preparation time for set up. Self-organization methods consist of routing algorithms that adapt to the dynamic changes and movements of the network nodes. However, in fast-changing networks, updates to the routing tables may leave little or no bandwidth for users to utilize the services of the network.

The dynamic, hierarchical aspects of ad hoc networking avoid the routing table problems by enabling group-wise peer management. This in turn allows the nodes to save power and allows the (sub) networks to manage their bandwidth better. For example, there is no reason for foot soldiers near a tank to be connected to a base-station on an UAV for network access. The tank's battery power and carrying power is far greater than that of the soldiers or the UAV. Instead, the UAV can provide point-to-point connectivity to the tank, and the tank can act as the central distributor to the soldiers. The network size, however, may dictate certain hierarchies that may be required for the management of these pseudo peer-to-peer networks, especially when the hierarchical military command is considered. Pure peer-to-peer or pseudo peer-to-peer topologies require robust routing protocols. The security implications, such as key management, are even more challenging to implement and manage in these types of topologies.

In [11], investigates a new class of self-organizing hierarchical ad-hoc wireless networks with improved scaling properties and integration that is more natural. The investigation was conducted using the Monarch extensions to the ns-2 network simulator. The proposed network architecture is based on three tiers of wireless devices: low-power/sensor nodes" with limited functionality, higher-power/radio forwarding nodes" that route packets between radio links, and access points" that route packets between radio links and the wired infrastructure.

8. Routing Protocols

Wireless military ad hoc networks require routing protocols that can dynamically adapt to the topology and hierarchical changes of the network nodes. Much of the research in this area is documented and criticized in Internet Engineering Task Force (IETF's) MANET Working Group [12]. Many routing algorithms are adapted from wired networks for the purposes of wireless ad hoc networking. However, the most interesting concept, which is unique to this field, is multi-hop routing capability.

This concept was developed for nodes or servers that have little or no access to the network. In such cases, access is made possible via other nodes in the vicinity. There

are cases where the lack of signal coverage dictates the forwarding of packets through several nodes. This multi-hop routing requires local routing table maintenance to include routing to all the nodes within a node's coverage area, and the sharing of updates periodically with them. The frequency of updates must match the node's coverage and environment, taking into consideration mobility and signal impairments. The method of updates, whether it is by broadcast or request, must match the network size and the intended QoS of the network. The overhead of the system is a compromise between channel resources and the routing protocol's efficiency.

C. SUMMARY

This chapter discussed the attributes of wireless networking concepts were discussed in relation to military necessity and observed previous work that researched these concepts with 802.11 technologies. These building blocks not only assist in defining the background assumptions of the design, but also the architecture's suitability for a tactical military situation. The next chapter will focus on the testing of the ES-520 and demonstrate its ability to act as a viable COTS solution for COASTS and other tactical environments.

IV. FORTRESS SECURE WIRELESS ACCESS BRIDGE (ES-520) PERFORMANCE AND ANALYSIS

A. INTRODUCTION

To accurately test the ES-520 network, procedures and methods were established. In this chapter, the evaluation process used to examine the ES-520 is discussed. A detailed outline of the methodology employed for testing, the reasons for the methodology, MOE and MOP, and the analysis of the findings, and how it would or would not apply to a tactical coalition operation are all examined. Additionally, the ES-520 network is discussed and the equipment configuration is presented.

B. AN OVERVIEW OF THROUGHPUT AND COVERAGE FACTORS

A WLAN generally consists of an access point (AP) that connects to a wired network and remote devices (client) that connect to the access point through wireless (radio) links. Throughput is defined as the speed with which a user can send and receive data between a remote device and the access point. Throughput varies across the WLAN's coverage area. This section profiles the main factors that determine WLAN throughput and coverage.

1. 802.11 Protocol

The IEEE 802.11 standard defines various physical-layer rates for different types of WLANs, such as 1, 2, 5.5 and 11 Mbps for 802.11b and 802.11g. Rates for 802.11a and 802.11g include 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. The user throughput is less than these link rates for several reasons:

1. Each packet includes additional data, such as preambles, headers (MAC, IP, Transmission Control Protocol (TCP), etc.) and checksums.
2. When every directed (unicast) packet is received, the receiver transmits a short acknowledge packet back to the sender.

3. Transmitters wait for short random times between packets to allow other users to contend for and share the channel [13].

Given these reasons, the theoretical maximum user-level performance for the various 802.11 systems is:

Number of Channels	Modulation	Maximum Link Rate		Maximum TCP Rate	Maximum UDP Rate
802.11b	3	CCK	11 Mbps	5.9 Mbps	7.1 Mbps
802.11g (with 11b)	3	OFDM/CCK	54 Mbps	14.4 Mbps	19.5 Mbps
802.11g (11g-only mode)	3	OFDM/CCK	54 Mbps	24.4 Mbps	30.5 Mbps
802.11a	19	OFDM	54 Mbps	24.4 Mbps	30.5 Mbps
802.11a TURBO	6	OFDM	108 Mbps	42.9 Mbps	54.8 Mbps

Table 1. Maximum Theoretical Performance for Various 802.11 Systems (From: [13].)

Table 1 assumes 1500-byte packets, encryption enabled, default 802.11 MAC configurations, zero packet errors, and maximum available channel bandwidth (that is, operating at close range). Note that some 802.11 implementations use tricks such as reducing back off times between packets to improve throughput performance. Such tricks can result in interoperability problems with other vendors' systems.

Table 1 also shows two rates for 802.11g to account for the lower rates in 802.11b compatibility mode. The throughput of an 802.11g WLAN decreases significantly in 802.11b compatibility mode because every 802.11g Orthogonal Frequency-Division Multiplexing (OFDM) packet needs to be preceded by a Clear-to-send (CTS) packet exchange recognizable by legacy 802.11b devices. With no 802.11b devices connected, an 802.11g network can operate in 11g-only mode and should achieve the standard throughput of 802.11a. The current 802.11g draft standard also provides for a slower Request-to-send (RTS)/CTS header (instead of CTS-only) when in 802.11b compatibility mode, which will further reduce the 14.4 Mbps TCP/IP rate to 11.8 Mbps [13].

You therefore have two choices with 802.11g networks: You can achieve high rates comparable with those of 802.11a networks. Or you can get 802.11b compatibility. You cannot have both at the same time.

Since the key feature of 802.11g is backward compatibility with 802.11b, throughput tests should be done with an 802.11b client device connected to the access point but otherwise idle. This setup ensures that the 802.11g network is operating in an 802.11b compatible mode.

2. The Radio Environment

Several issues affect the way the radio signal travels from one device to another:

1. Radio energy attenuates when it propagates. As radio waves propagate outwards spherically, the energy spreads over an ever-increasing area. In free space, doubling the distance decreases the received power by a factor of 4—the so-called $1/r^2$ behavior. Radio signals also attenuate when they pass near or through objects such as floors, walls, furniture, and people. The attenuation increases with the object's conductivity (due to metal or water content, for example). The combination of these two attenuation effects reduces radio signal strength by $1/r^3$ to $1/r^4$, or even $1/r^5$. In other words, each time you double the distance, the received power might decrease by 8 to 16 times.
2. Antenna design affects how much RF energy is transmitted or received and where it is directed.
3. Scattering and multi-path cause fading effects. Signal strength can change rapidly as a function of location because the received signal is the sum of potentially numerous signals scattered from nearby objects. As the transmitter or other objects in the environment move, the scattered signals sometimes add together and sometimes cancel each other. Fading can change significantly over distances of a wavelength or so (12.5 centimeter (cm) at 2.4 Gigahertz (GHz) and 6 cm at 5

GHz). Fading also occurs over time as well as location. Even small changes in the environment (for example, people or other objects moving) can affect the fading pattern. This means that the received signal strength can also change quite quickly over time, even when the receiver and transmitter are fixed.

4. Scattering and multi-path results in delay spread. The received signal might contain several slightly delayed copies of the transmitted signal, as the scattered signals travel via different physical paths of different lengths.
5. Other devices occupying the same or nearby channels cause interference. For example, the 2.4 GHz spectrum might be occupied by Bluetooth devices, microwave ovens, and cordless telephones [13]

3. Frequency

A common misconception is that free-space propagation depends upon frequency, so higher frequencies are assumed to propagate less well than lower frequencies. As a good counter example to this misconception, consider visible light, which is simply an ultra-high frequency electromagnetic wave that propagates perfectly well across large distances.

On the other hand, effects such as antenna efficiency, RF component performance, and absorption through and scattering around objects do depend upon frequency. Here are some of the frequency-dependent effects:

1. Generally, antennae of the same physical size tend to become more directional (have higher gain in some directions and less in others) as the frequency increases. Advantage: 5 GHz.
2. Absorption due to propagation through objects tends to increase with frequency. Advantage: 2.4 GHz.

3. Scattering around objects might have a positive or negative effect on signal strength as a function of frequency, depending upon the relative sizes and locations of the objects. Advantage: Neutral.
4. Noise and spurs generated by nearby electronics (for example, inside the AP or Personnel Computer (PC) laptop) in addition to co-channel interference, such as Bluetooth devices, cordless phones and microwave ovens, will degrade 2.4 GHz sensitivity more than 5 GHz. Advantage: 5 GHz.
5. Cable loss increases with frequency, so antenna cables (if present) in the AP or laptop will have more loss at high frequency, unless more expensive cables are used. Advantage: 2.4 GHz [13].

Typically, the OFDM modes of 2.4 GHz 802.11g networks will have slightly less coverage than 2.4 GHz 802.11b networks. Depending upon the propagation environment, the coverage of 5 GHz 802.11a networks might be similar to, or in some cases less than, that of 802.11g networks. The differences between 2.4 and 5 GHz propagation are generally insignificant compared to the differences between one vendor's equipment and another's, however. An 802.11a product from one vendor might have better coverage than an 802.11g product from another vendor.

4. The Vendor Equipment Design

Equipment from different vendors exhibit significantly different performances due to architecture, design, manufacturing and software variations, as well as proprietary features and enhancements.

5. Vendor Interoperability

Products that undergo Wi-Fi certification are certified to interoperate with a wide variety of vendors' products. However, these tests mainly verify basic connectivity and do not enforce stringent throughput requirements. You might be able to connect a client device to a different vendor's access point, but you might not be getting very high

throughput. Products that provide good performance (throughput, coverage, etc.) when connected to a variety of different vendor's devices are clearly more desirable.

6. Security

Security includes encryption and authentication. Encryption protects WLAN traffic from eavesdropping and other attacks such as replay or man-in-the-middle attacks. Authentication validates the users' credentials (ensuring that the user is who they say they are) and possibly validates the network's credentials (ensuring that the network is what it says it is, and not someone masquerading as the network).

WLAN security standards have progressed from Wired Equivalent Privacy (WEP) to Temporal Key Integrity Protocol (TKIP) and Wi-Fi Protected Access (WPA) and now to AES, with significant security enhancements at each stage. No matter what security standard is involved, the way the standard is implemented can affect the WLAN's performance. Specifically, some vendors implement encryption in software, which can dramatically reduce throughput compared to advertised rates. When evaluating performance, it is vital to measure throughput with encryption enabled [13].

C. MEASURING THROUGHPUT AND COVERAGE

The throughput of WLANs depends heavily on the environment, including the distance between the client and the access point. The throughput generally falls off as distance increases, but factors such as obstructions (like furniture, people, or walls of different construction) also have a significant effect. Throughput does not depend upon distance alone. It is possible to have distant test locations that produce higher data rates than closer locations. Moreover, the peak data rate measured at short distances is not the most important factor in the user's experience. Rather, the rate the user experiences at a variety of distances and locations is a very important factor. Therefore, it is critical to measure WLAN throughput at a variety of locations, including some far from the access point.

WLAN environments generally fall into three categories:

1. Outdoor: typically a direct line of sight between the access point and client. Examples include outdoor campus coverage, public areas, or even inside large, open buildings such as airport concourses or convention halls.
2. Open office: no longer a direct line of sight between the access point and client, but typically at most two-to-three obstructions such as walls. Examples are warehouses or offices containing cubicles, lobbies and meeting areas.
3. Closed office: no direct line of sight, with many obstructions between the access point and the client. Examples are buildings with regular offices and many walls [13]

WLAN coverage differs significantly in these different environments. Outdoor WLANs provide the longest ranges and closed-office WLANs the shortest. Different construction techniques also have a significant impact on coverage and throughput. For instance, concrete walls attenuate signals more than stud walls with sheet rock. In general, the relative performance and throughput for different products under test should be similar across the different environments. So if Vendor #1's product is significantly better than Vendor #2's in an open-office environment, it is highly likely (although not guaranteed) that it will be significantly better in other environments. It is possible (although more time consuming) to test products across several different environments to accurately determine the relative performance.

D. ES-520 NETWORK SUPPORTING HARDWARE AND SOFTWARE

To evaluate the performance of the ES-520 network, an extensive amount of supporting hardware and software was used in this research. These include the 3COM switch, West Marine battery, PowerBright power inverter, Garmin Foretrex 201, the “Google Earth” application, antennas, laptop computers, and the test application,

“IxChariot.” Each of the supporting hardware and software are discussed in the Appendix ES-520 Network Supporting Hardware and Software Specifications.

E. MEASURES OF EFFECTIVENESS AND PERFORMANCE

MOE’s represent the customer view, usually annotated and of qualitative nature. They describe the customers’ expectations of a product, project or system; the voice of the customer. MOP’s are the corresponding view of the engineer. Typically, MOP’s are quantitative and consist of a range of values about a desired point. These values are what an engineer targets when designing the product, by changing shape, materials and manufacturing process, to achieve the qualities desired by the customer. Both the MOE and MOP can be constructed as a hierarchy diagram, with weighted values for each metric, and can be displayed horizontally or vertically. Each level of the hierarchy represents 100% of the effectiveness or performance [14].

Using MOE’s and MOP’s proves to be useful when evaluating complex systems. The use of MOE’s supports the military commander decision-making when deciding on the best quality COTS product to use in the battlespace, while MOP’s provide the military commander a quantitative view on what to expect from the COTS product. Additionally, the use of MOE’s and MOP’s promotes making objective decisions when comparing more than one system.

1. Selected MOE and MOP

The selection of MOE and MOP was based on the needs of the COASTS 2007 scenario and experiments. This section describes the developed MOE and MOP for the ES-520 network.

a. 802.11 Network - ES-520 MOE

The selected metrics for MOE are as follows: support of land platforms, support of data, easily configurable, immediately available for purchase, and operational availability. Support of land platforms can best be described as the ability of the network

work in dense vegetation. Support of data is the ability for the network to effectively pass data in real-time. Easily configurable suggests that operators will quickly learn how deploy the system. Immediately available for purchase means that all parts associated with setting up the network can be purchased in a timely manner. Operational availability is the amount of time the system is running opposed to the amount of time it is not running. Figure 1 depicts the selected MOE.

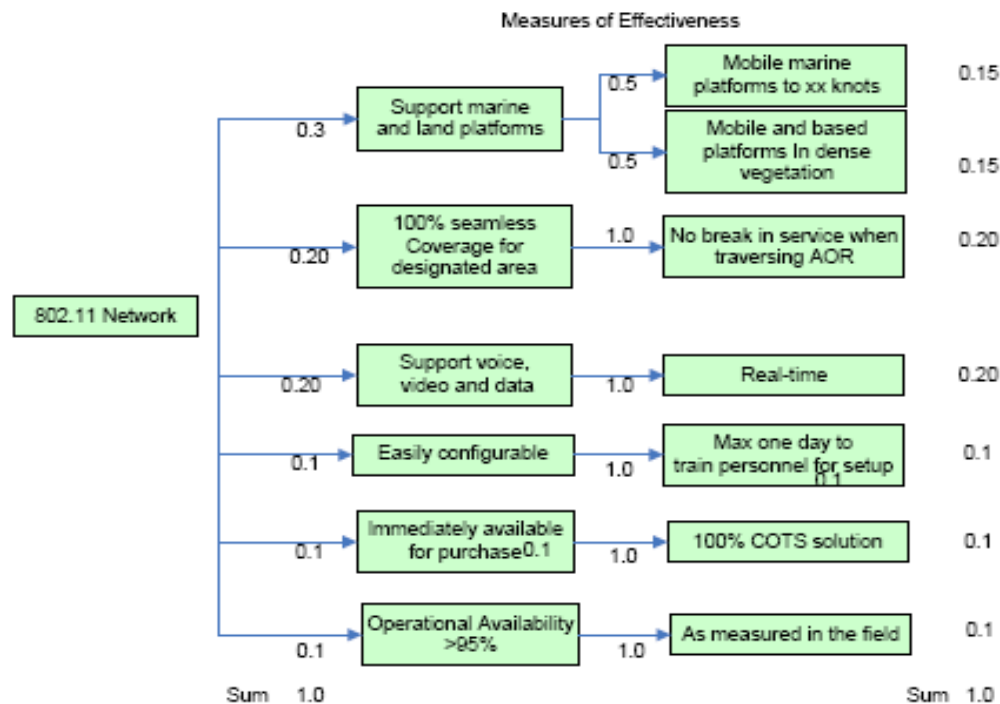


Figure 1. Selected ES-520 MOE

b. 802.11 Network - ES-520 MOP

The selected metrics MOP are as follows: throughput, transaction rate, and response time. In order to retrieve this from the ES-520 network, the test application IxCahriot from IXIA was used. IxChariot was chosen mainly for its ease of use and reputation as being one of the best software tools available for monitoring and analysis of networks. IxChariot was used with the throughput.scr script. The throughput.scr script is recommended for testing maximum throughput on typical networks. Additionally, results

for transaction rate and response time are displayed with the throughput.scr script. This script was adjusted to send 100 packets between each endpoint pair. It then waited for an acknowledgment. The script thus simulated the core file transfer transaction performed by many demanding audio and video applications.

Throughput is the measure of the amount of data (bits or bytes/second) that can be sent through a network. It is a useful performance indicator for file transfer and multimedia applications. IxChariot calculates throughput by the formula: $\text{Throughput} = ((\text{Bytes Sent} + \text{Bytes Received}) / \text{Throughput Units}) / \text{Measured Time}$. Bytes Sent is the number of bytes sent by endpoint 1 of a pair. Bytes received are the number of bytes received by Endpoint 1 of a pair. Throughput units are the current throughput unit's value, in bytes per second. For all tests, throughput units were Mbps, which is 125,000 bytes per second.

The transaction rate is the number of script transactions that are executed per second. IxChariot calculates transaction rate by the formula: $\text{Transaction rate} = \text{Transaction Count} / \text{Measured Time}$

Response time is the measure of the end-to-end round-trip time required to complete an application-level transaction across the network. Response time is the most effective performance indicator of human-computer interaction. IxChariot calculates response time by the formula: $\text{Response Time} = \text{Measured Time} / \text{Transaction Count}$. Measured time is the time, in seconds, taken to complete all the transactions for a given connection pair. The transaction count is the number of transactions completed by Endpoint 1. Figure 2 illustrates the selected MOP.

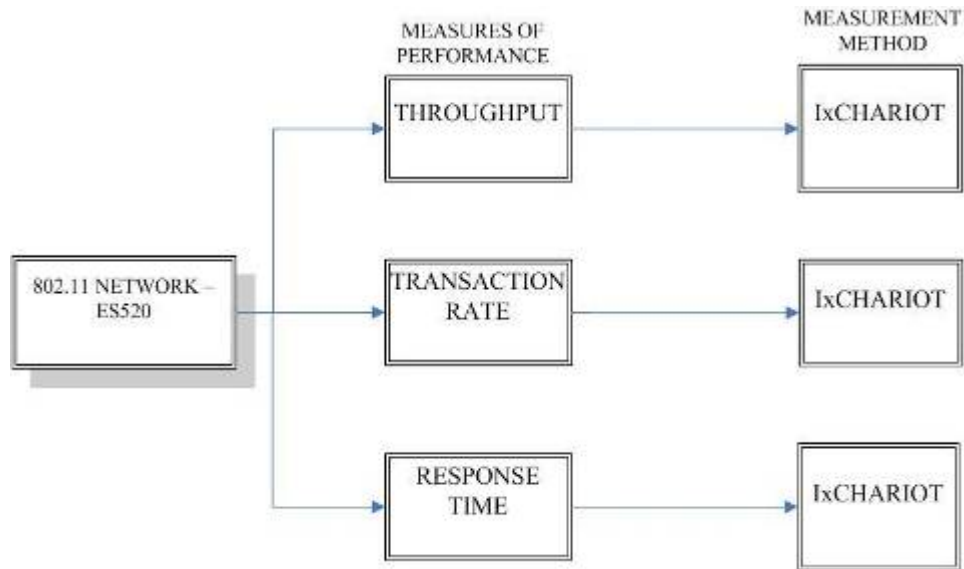


Figure 2. Selected ES-520 MOP

2. Controllable Factors

Several controllable factors are expected to influence the MOE. These factors include, but are not limited to sensor sensitivity, sensor elevation, object type, object speed, and environmental conditions.

Controllable factors expected to affect MOP are discussed next. Factors affecting throughput are sensor sensitivity, sensor elevation, object type, object speed, and environmental conditions. Transaction rate is affected by protocol overhead, retransmission of lost or corrupt packet, and collision detection in the Carrier Sense Multiple Access With Collision Detection (CSMA/CD) protocol. Response time controllable factors are distance, weather, transmission power, receiver sensitivity, sensor elevation, terrain, and environmental conditions.

Wireless networks need a clear signal path to operate. This not only means visual line of sight, but also radio line of sight. Visual line of sight is the straight line connecting any two nodes. While it is possible for the signal to propagate along this line, optimally a complete clear radio line of sight is preferred. Radio line of sight takes into account the shape of the zone that the radio waves travel in. This is called the “Freznel” zone. In

other words, the radio waves travel between the nodes covering an elliptical area and so the clearance desired halfway between the nodes is greater than at each node location.

Therefore, to achieve a near optimal signal path, nodes must be spaced at elevated locations such as hilltops, tall buildings and others. The strength of the signal is a good indicator of correct placement. In the case of this research, locations were surveyed before final placement. With these considerations in mind, the root node was placed at or nearby a highly elevated location and connected with a wired network. The non-root nodes were mounted in similar locations.

F. FIELD EXPERIMENTS

1. Basis

To test the proposed solution, it was necessary to: 1) Simulate actual conditions, and 2) Perform tests. Simulating actual conditions was needed to study the applicability and limitations of long-range use of the ES-520 when applied to a Command and Control (root) node – remote (non-root) node. Based on this choice, the selection of the site depended on the military sites that COASTS use for field experimentation. The main criteria for this selection were distance and LOS.

As previously stated, the research focuses on testing the ES-520 for maximum distance, while maintaining adequate throughput, transaction rate, and response time. The test is conducted with the purpose of simulating a military unit deploying the ES-520 to receive information from a command center. The testing was conducted during two test experiments by COASTS at Camp Roberts (CR) and Fort Hunter Liggett (FHL). The first occurred in December of 2006 and the second in January of 2007. The equipment setup and test results were captured during periods scheduled specifically for experimentation, and at other times as available. The network configuration and equipment setup are presented below.

2. ES-520 Network Operating Areas

In December of 2006, the first field experiment was done at McMillan Airfield on CR. In Figure 3 the root-node, location $35^{\circ}42'56.61''\text{N}$ $120^{\circ}45'50.53''\text{W}$, is illustrated along with the positions of the non-root nodes.



Figure 3. CR Operating Area

In January of 2007, another field experiment was conducted at the Schoonover Assault Strip on FHL. The root-node, location $35^{\circ}58'13.40''\text{N}$ $121^{\circ}11'59.30''\text{W}$, along with the non-root nodes are depicted in Figure 4 and 5.



Figure 4. FHL Client Test Operating Area



Figure 5. FHL Operating Area

3. ES-520 Network Configuration

The entire COASTS network was configured as a static IP network. The various nodes were assigned an IP space, an appropriate subnet mask, and gateway for the duration of the tests. They are presented in Table 2 below.

Node Name: IP Address/Subnetmask		Gateway
ES-520 Network: 192.168.10.0/255.255.255.0		192.168.10.254
Date: 01 DEC 06		
Address	Node Name	
192.168.10.94	Root Endpoint Laptop	
192.168.10.72	Non-root Endpoint Laptop	
192.168.10.28	Root ES-520	
192.168.10.25	Non-root ES-520	
192.168.10.26	IxChariot Laptop	
192.168.10.250	3Com Switch	
Date: 02 DEC 06		
192.168.10.94	Root Endpoint Laptop	
192.168.10.72	Non-root Endpoint Laptop	
192.168.10.28	Root ES-520	
192.168.10.25	Non-root ES-520	
192.168.10.26	IxChariot Laptop	
192.168.10.250	3Com Switch	
Date: 17 JAN 07		
192.168.10.35	Root Endpoint Laptop	
192.168.10.20	Non-root Endpoint Laptop	
192.168.10.28	Root ES-520	
192.168.10.25	Non-root ES-520	
192.168.10.26	IxChariot Laptop	
192.168.10.250	3Com Switch	
Date: 18 JAN 07		
192.168.10.35	Root Endpoint Laptop	
192.168.10.20	Non-root Endpoint Laptop	
192.168.10.28	Root ES-520	
192.168.10.25	Non-root ES-520	
192.168.10.26	IxChariot Laptop	
192.168.10.250	3Com Switch	

Date: 19 JAN 07		
192.168.10.35	Root Endpoint Laptop	
192.168.10.20	Non-root Endpoint Laptop	
192.168.10.28	Root ES-520	
192.168.10.25	Non-root ES-520	
192.168.10.26	IxChariot Laptop	
192.168.10.250	3Com Switch	
Date: 20 JAN 07		
192.168.10.35	Root Endpoint Laptop	
192.168.10.20	Non-root Endpoint Laptop	
192.168.10.28	Root ES-520	
192.168.10.26	IxChariot Laptop	
192.168.10.250	3Com Switch	

Table 2. ES-520 Network IP Addresses, Sub Masks, and Gateways

The address space allocated to the testing of the ES-520 network is within the 192.168.10.0 Class C address with a subnet mask of 255.255.255.0. The laptops themselves are shown below in Figure 6 and 7.



Figure 6. IxChariot Laptop and Root Endpoint Laptop used for ES-520 Network Testing



Figure 7. Non-root Endpoint Laptop used for ES-520 Network Testing

The laptops in Figure 6 were set up in the Tactical Operations Center (TOC) at each location. The laptop in Figure 7 was taken to each non-root site and setup for operation. In Figure 8, one can see the laptop configured for the ES-520 experimentation at a non-root node site.



Figure 8. Non-root ES-520 Setup

Overall, a basic network diagram is presented in Figure 9 for the ES-520 WLAN. This simplified version offers a clear view of the testing platform.

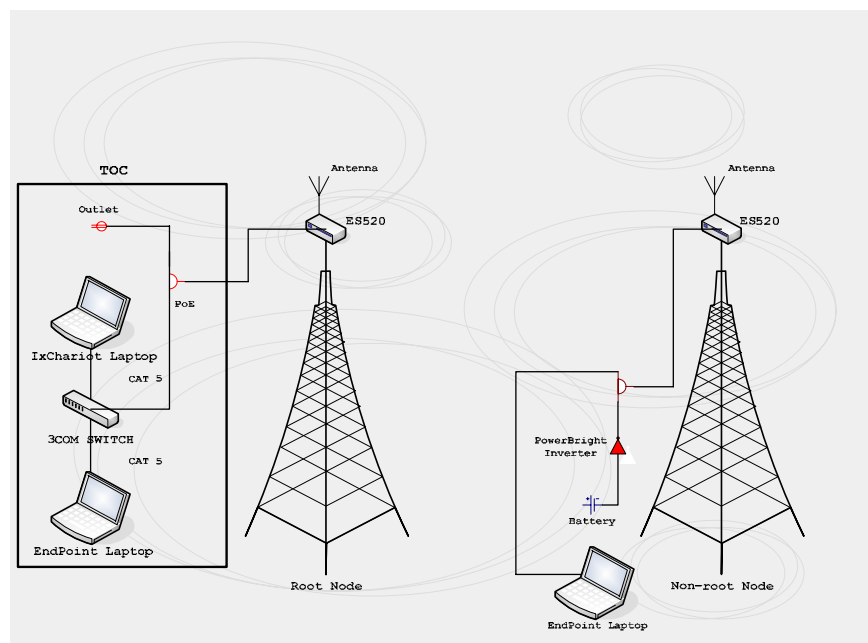


Figure 9. Basic ES-520 Network Diagram

4. ES-520 Equipment Configuration

The ES-520 root and non-root nodes were configured using the GUI interface supplied with the units. Table 3 gives the MAC addresses for each piece of equipment used in the experiment.

Component	MAC
3Com Switch	00-18-6E-C6-46-93
ES-520 Root node	02-14-8C-08-31-42
ES-520 Non-root node	02-23-7E-09-42-63
Root Endpoint Laptop	00-12-3F-1A-80-B2
Non-root Endpoint Laptop	00-13-02-34-03-F0
IxChariot Laptop	00-14-22-D0-51-D8

Table 3. Component MAC Addresses

G. RESULTS

Performance results were gathered using the IxChariot application. The settings for each test, called the run options, are described. The endpoint pair configurations, referred to as the test setup, are detailed. In addition, the throughput, transaction rate, and response time for each test are given for the system under a common load.

1. Run Options

The run options for each test were the same, with the exception of the run duration. The run duration for each test is given in the description of the tests in the next section. All tests used the same settings are listed in Table 4.

End type	Run until any pair ends
Reporting type	Real-time
Automatically poll endpoints	Yes
Polling interval (minutes)	1
Stop run upon initialization failure	Yes
Connect timeout during test (minutes)	0
Stop test after this many running pairs fail	1

Collect endpoint CPU utilization	No
Collect TCP statistics	No
Allow pair reinitialization for setup	No
Maximum number of setup reinitializations	3
Setup reinitialization wait interval (milliseconds)	10
Allow pair reinitialization at runtime	No
Maximum number of runtime reinitializations	3
Runtime reinitialization wait interval (milliseconds)	10
Validate data upon receipt	No
Use a new seed for random variables on every run	Yes
Enable Ixia hardware timestamps	Yes
Clock synchronization	'Endpoint'

Table 4. Run Options

2. Test Setup

The ES-520 was scheduled to be tested in two locations. The goal of the experiment was to test the equipment limits in terms of distance and LOS. Specifically, both bridges were mounted and the bandwidth was tested under several configurations of the distance, terrain elevations (LOS), and different Omni-directional antennas.

a. Camp Roberts (CR)

The following tests were conducted between December 1 and December 2, 2006. The physical network configuration was as shown in Figure 19. During each test, one endpoint pair was evaluated over the ES-520 network. The pair was 192.168.10.94:192.168.10.72. All points at Camp Roberts were LOS. Table 5 describes the distance between nodes and elevation difference.

Test Setup		
Test Point	Distance from Root node (meters)	Elevation Difference Between Root Node and Non-root Node (meters)
CR Point 1	853.59	27↑
CR Point 2	1132.55	59↑
CR Point 3	1470.48	67↑

CR Point 4	1459.66	76↑
CR Point 5	281.47	1↓
CR Point 6	547.69	0
CR Point 7	873.29	6↑
CR Point 8	1385.98	68↑
*Note CR Root node was at an elevation of 274 meters. Up and Down arrows, indicate whether Non-root nodes were above or below Root node.		

Table 5. Camp Roberts Distance Between Nodes and Elevation Difference

b. Fort Hunter Liggett (FHL)

The following tests were conducted between January 16 and January 20, 2007. The physical network configuration was as shown in Figure 19. During each test, one endpoint pair was evaluated over the ES-520 network. The pair was 192.168.10.35:192.168.10.20. FHL Client Point 1, FHL Point 2, and FHL Point 4 were non-LOS and were through light density vegetation. FHL Client Point 2 and FHL Point 3 were non-LOS and were through medium density vegetation. The remaining points were LOS. Table 6 describes the distance between nodes and elevation difference.

Test Setup		
Test Point	Distance from Root node (meters)	Elevation Difference Between Root Node and Non-root Node (meters)
FHL Client Point 1	53	2↑
FHL Client Point 2	124.62	1↓
FHL Client Point 3	113.97	3↓
FHL Client Point 4	167.52	3↓
FHL Point 1	1458.3	10↓
FHL Point 2	1095.29	5↑
FHL Point 3	790.03	2↑
FHL Point 4	1299.12	22↑

*Note FHL Root node was at an elevation of 293 meters. Up and Down arrows, indicate whether Non-root nodes were above or below Root node.

Table 6. Fort Hunter Liggett Distance Between Nodes and Elevation Difference

3. ES-520 Measures of Performance

a. Camp Roberts

CR Points one to eight were used for field data collections. Table 7 summarizes the results collected at Camp Roberts.

Antenna Configuration	Throughput (Mbps)			Transaction Rate			Response Time (seconds)		
	Minimum	Average	Maximum	Minimum	Average	Minimum	Minimum	Average	Maximum
SuperPass to SuperPass									
CR Point 1	4.79	12.682	19.512	5.988	16.062	24.39	0.041	0.062	0.167
CR Point 2	2.797	13.349	20.513	3.497	16.686	25.641	0.039	0.06	0.286
CR Point 3	4.819	13.221	19.512	6.024	16.526	24.39	0.041	0.061	0.166
CR Point 4	5.517	13.671	19.512	6.897	17.088	24.39	0.041	0.059	0.145
CR Point 5	10.959	19.075	24.243	13.699	23.844	30.303	0.033	0.042	0.073
CR Point 6	17.201	10.39	22.857	12.987	21.501	28.571	0.035	0.047	0.077
CR Point 7	4.79	12.849	19.512	5.988	16.062	24.39	0.041	0.062	0.167
SuperPass to 12dBi									
CR Point 1	3.213	7.572	14.035	4.016	9.465	17.544	0.057	0.106	0.249
CR Point 2	1.011	6.144	11.94	1.264	7.68	14.925	0.067	0.13	0.791
CR Point 3	1.684	6.96	14.035	2.105	8.699	17.544	0.057	0.115	0.475
CR Point 4	1.375	6.721	13.559	1.718	8.401	16.949	0.119	0.059	0.582
CR Point 8	0.668	5.966	16	0.835	7.457	20	0.05	0.134	1.197
12dBi to 12dBi									
CR Point 1	2.279	7.219	11.111	2.849	9.024	13.889	0.072	0.111	0.351
CR Point 2	3.292	8.076	15.686	4.115	10.095	19.608	0.051	0.099	0.243
CR Point 3	1.282	6.279	11.765	1.603	7.848	14.706	0.068	0.127	0.624
CR Point 4	1.246	6.718	13.115	1.558	8.398	16.393	0.061	0.119	0.642
CR Point 8	3.604	7.32	12.699	4.505	9.15	15.873	0.063	0.109	0.222

Table 7. Camp Roberts Throughput, Transaction Rate, and Response Time Results

Looking at maximum data throughput from Camp Roberts, it shows that the 8dBi SuperPass antenna was the best configuration. The maximum throughput

average was 20.81 Mbps. CR Point 5 was the closest point and had the highest maximum throughput. Additionally, the requirement for the COASTS program is 20 Mbps maximum throughput. CR Points 1, 3, 4, and 7 were at 19.512 Mbps, just below the requirement. The closest point where throughput drops below 20 Mbps is CR Point 1 with a distance of 853.59 meters.

b. Fort Hunter Liggett

FHL Points one to four were used for field data collections of 5.8 GHz antennas and FHL Client Points one to four represent the 2.4 GHz antennas. Table 8 summarizes the results collected at Camp Roberts.

Antenna Configuration	Throughput (Mbps)			Transaction Rate			Response Time (seconds)		
	Minimum	Average	Maximum	Minimum	Average	Maximum	Minimum	Average	Maximum
2.4GHz, 7dBi to Laptop									
FHL Client Point 1	1.039	17.131	21.042	0.013	0.214	0.263	3.802	4.67	77.007
FHL Client Point 2	4.613	5.8	16.974	0.058	0.072	0.212	4.713	13.794	17.344
FHL Client Point 3	0.713	5.95	13.057	0.009	0.074	0.163	6.127	13.445	112.259
FHL Client Point 4	4.562	12.562	17.101	0.057	0.157	0.214	4.678	6.368	17.536
SuperPass to SuperPass									
FHL Point 1									
Run 1	1.587	13.093	19.048	1.984	16.367	23.81	0.042	0.061	0.504
Run 2	1.743	14.383	19.048	2.179	17.979	23.81	0.042	0.056	0.459
Run 3	10.127	16.149	20	12.658	20.186	25	0.04	0.05	0.079
Run 4	2.388	15.086	20	2.985	18.857	25	0.04	0.053	0.335
Run 5	9.723	16.844	18.935	0.122	0.211	0.237	0.122	0.211	0.237
FHL Point 2									
Run 1	7.692	12.432	15.094	9.615	15.54	18.868	0.053	0.064	0.104
Run 2	2.508	12.291	15.385	3.135	15.363	19.231	0.052	0.065	0.319
Run 3	1.536	10.189	15.686	1.919	12.736	19.608	0.051	0.079	0.521
Run 4	2.326	12.112	15.686	2.907	15.14	19.608	0.051	0.066	0.344
Run 5	1.078	11.493	15.686	1.348	14.366	19.608	0.051	0.07	0.742
Run 6	1.426	11.46	15.094	1.783	14.325	18.868	0.053	0.07	0.561
Run 7	10.721	12.925	14.493	0.134	0.162	0.181	5.52	6.19	7.462
FHL Point 4									
Run 1	2.286	14.461	20	2.857	18.077	25	0.04	0.055	0.35
8dBi to 8dBi									
FHL Point 3									
Run 1	1.643	15.086	20	2.053	18.857	25	0.04	0.053	0.487
Run 2	1.495	14.931	20	1.869	18.664	25	0.04	0.054	0.535

Run 3	1.515	15.106	20.513	1.894	18.882	25.641	0.039	0.053	0.528
Run 4	1.541	14.809	19.512	1.927	18.512	24.39	0.041	0.054	0.519
Run 5	17.116	19.014	19.891	0.214	0.238	0.249	4.022	4.208	4.674
FHL Point 4									
Run 1	1.544	14.749	21.053	1.931	18.437	26.316	0.038	0.054	0.518
10dBi to 10dBi									
FHL Point 1									
Run 1	10.257	14.422	19.048	12.821	18.028	23.81	0.042	0.055	0.078
Run 2	11.111	14.561	17.391	13.889	18.202	21.739	0.046	0.055	0.072
Run 3	1.416	12.285	16.327	1.77	15.356	20.408	0.049	0.065	0.565
Run 4	1.401	12.697	18.605	1.751	15.87	23.256	0.043	0.063	0.571
Run 5	13.652	14.725	16.824	0.171	0.184	0.21	4.755	5.433	5.86
FHL Point 2									
Run 1	3.2	15.302	20	4	19.128	25	0.04	0.052	0.25
Run 2	1.695	13.555	19.512	2.119	16.943	24.39	0.041	0.059	0.472
Run 3	1.351	14.263	19.512	1.689	17.828	24.39	0.041	0.056	0.592
Run 4	1.569	14.363	20	1.961	17.953	25	0.04	0.056	0.51
Run 5	1.083	13.867	20.513	1.353	17.334	25.641	0.039	0.058	0.739
Run 6	2.26	15.311	22.222	2.825	19.139	27.778	0.036	0.052	0.354
Run 7	16.481	18.178	19.394	0.206	0.227	0.242	4.125	4.401	4.854
FHL Point 4									
Run 1	1.487	12.074	16	1.859	15.092	20	0.05	0.066	0.538
12dBi to 12dBi									
FHL Point 1									
Run 1	6.667	12.037	14.815	8.333	15.047	18.519	0.054	0.066	0.12
Run 2	1.368	10.788	14.815	1.709	13.484	18.519	0.054	0.074	0.585
Run 3	1.471	10.882	14.546	1.838	13.602	18.182	0.055	0.074	0.544
Run 4	2.168	11.22	15.094	2.71	14.025	18.868	0.053	0.071	0.369
FHL Point 2									
Run 1	4.445	9.186	13.335	55.556	114.811	166.667	0.006	0.009	0.018
FHL Point 4									
Run 1	1.518	11.693	15.686	1.898	14.616	19.608	0.051	0.068	0.527

Table 8. Fort Hunter Liggett Throughput, Transaction Rate, and Response Time Results

The FHL Client Points were conducted with only one 2.4 GHz antenna. Therefore, a statement on which configuration is best cannot be made. However, maximum throughput averaged 17.04 Mbps among the four points. FHL Client Point 1 received the highest throughput of 21.042 at 53 meters. As previously stated, FHL Client Point 1 was through light density vegetation.

Looking at maximum data throughput from FHL with 5.8 Ghz antennas, it shows that the 10dBi HyperLink antenna was the best configuration with a maximum throughput average was 20.16 Mbps. The highest maximum throughput of 22.22 Mbps was received at FHL Point 2 at a range of 1095.29 meters. FHL Point 2 was through medium density.

H. ANALYSIS

The ES-520 did not perform as expected during the experiments demonstrated in December 2006 and January 2007. The ES-520's capabilities proved to be not as advertised. However, one must objectively evaluate ES-520 based upon the metrics, MOP, and MOE discussed in previous chapters.

The support to land platforms was worth 30 percent of the ES-520's evaluation. In this area, the ES-520 was only given 20 out of 30 because of the significantly lower throughput if the experiment was not direct LOS. The 100% seamless coverage for designated area was worth 20 percent of the total evaluation. The ES-520 did provide 100% coverage, therefore 20 points was given. Support of voice, video, and data was worth 20 percent of the evaluation. As demonstrated by the throughput.scr of IXIA, the ES-520 did support voice, video, and data. Thus, 20 points was given in this area. Easily configurable was worth 10 percent. Easily configurable received the maximum points of 10. Immediately available for purchase was worth 10 percent and operational availability was worth 10 percent. 100% COTS solution was given a maximum amount of point worth 10 points and 10 points for immediately available. When compared to the MOE, the ES-520 was given a total of 90 out of 100 points.

In regards to MOP, the ES-520 did well in transaction rate and response time. However, throughput did not meet the needs of COASTS. This can be best be attributed to the use of Omni-directional antennas. If directional antennas were used, one could reasonably expect throughput to be higher. Given that this experiments purpose was for maximum distance and LOS to simulate military units receiving information from command center as if setting up a temporary station, the results received are acceptable.

I. SUMMARY

This chapter provided the procedures and methods were established to conduct the testing of the ES-520. A detailed outline of the methodology employed for testing, the reasons for the methodology, MOE and MOP, and the analysis of the findings, and how it would or would not apply to a tactical coalition operation was provided. Additionally, the ES-520 network is discussed and the equipment configuration is presented.

V. FEASIBILITY, SUSTAINABILITY, AND TECHNICAL ADVANTAGES/DISADVANTAGES OF THE FORTRESS SECURE WIRELESS ACCESS BRIDGE (ES-520)

A. BACKGROUND

COTS offer the promise of technology advancement, low cost and reduced acquisition time. Unfortunately, it also offers the opportunity for a reliability and logistics disaster because commercial parts, standards, and practices may not meet military requirements. Additionally, commercial vendors have little or no experience in providing the kind of technical data required to support military deployment logistics.

COTS hardware is expected to have the following characteristics; low cost, currently available from multiple suppliers, built to documented standards in high volume production with a mature design. This chapter offers some guidance in the selection of the ES-520 based on feasibility, sustainability, and technical advantages and disadvantages.

B. FEASIBILITY OF THE ES-520

The rationale for using COTS is that they will involve less development time by taking advantage of existing, market proven, vendor-supported products, thereby reducing overall system development costs. However, because of lack of access to product source code and lack of control over product evolution, there is a trade-off in using the COTS approach in that development time can indeed be reduced, but generally at the cost of an increase in component integration work. Moreover, using COTS also brings with it a host of unique risks quite different from those associated with military specific products.

Included among those risks or factors which should be examined when determining the true cost of integrating COTS larger system are not only the traditional costs associated with new software development such as the cost of requirements, definition, design, test, and maintenance, but also the cost of licensing, royalties, effort

needed to understand the COTS product, pre-integration assessment and evaluation, post-integration certification of compliance with mission critical or safety critical requirements, indemnification against faults or damage caused by vendor supplied components, and costs incurred due to incompatibilities with other hardware [15].

Because of these unique risks, using COTS products in the development of new systems is not the universal solution to reducing cost and schedule while maintaining desired quality and functionality. However, if these risks can be managed, using COTS product can frequently be the right solution, offering the most cost-effective, shortest schedule approach to assembling major systems.

COTS products are the right solution when they lie at the intersection of the three determinants of feasibility--technical, economic, and strategic constraints--and do so in a way demonstrably better than if a new system were to be constructed entirely out of a new military product (Figure 10). The key to success in using COTS products is being able to identify whether they fit the current procurement situation--technically, economically, and strategically. Technically, they have to be able to supply the desired functionality at the required level of reliability. Economically, they have to be able to be incorporated and maintained in the new system within the available budget and schedule. Strategically, they have to meet the needs of the system-operating environment--which includes technical, political, and legal considerations--now, and as that environment is expected to evolve in the future.

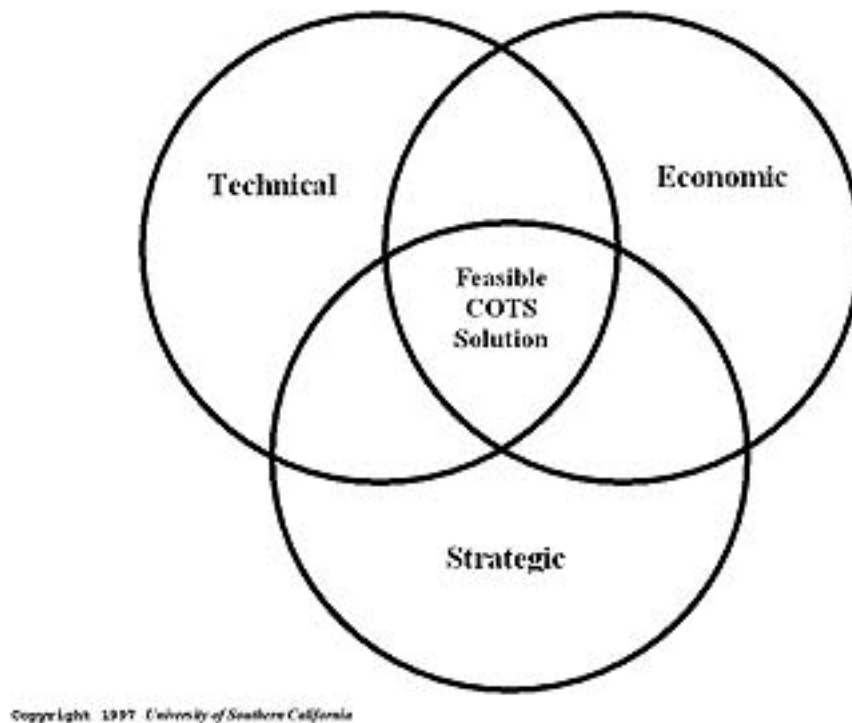


Figure 10. The Determinants of COTS Component Feasibility: Technical, Economic, and Strategic Constraints. (From: [15].)

Technical and strategic feasibility is determined during the candidate assessment phase of procuring COTS products, which occurs at the start of a COTS integration activity. How to determine the viability of a COTS product in either of these two dimensions is not a trivial question, and can be partially addressed by using the Constructive COTS (COCOTS) Assessment sub model. However, it is the third dimension of determining economic feasibility, which is the main intended use of COCOTS [15].

To answer the question of economic feasibility, cost estimation models exist which capture the traditional costs associated with new software development noted above, among the most prominent being Constructive Cost Model (COCOMO). To date, however, very few estimation models have been developed which try to capture those other costs unique to using COTS components in system development. The number of COTS integration cost models available in the public domain currently approaches zero.

In response to this situation, University of Southern California-Center for Systems and Software Engineering (USC-CSE) has been actively pursuing COTS integration cost modeling research since 1995. The most recent result of this research is COCOTS (Constructive COTS), a cost estimation model designed to capture explicitly the most important costs associated with COTS product integration [15].

Based on the previous section, the ES-520 was considered for feasibility by technical, economic, and strategic aspects. First, when considering feasibility, the following questions arise:

1. Can current technology be upgraded or added to?
2. Is particular technology available?

Based on the description of the ES-520 and research conducted, the ES-520 can be upgraded by the implementation of firmware and software upgrades. Additionally, the research and the current use of the ES-520 in COASTS show that the technology is currently available.

The second consideration of economy can be answered by the following questions:

1. How much time is needed from analysts, team members, and users?
2. How much is the cost of a full systems study?
3. How much is the cost of hardware?
4. How much is the cost of software?

To answer the questions about time, a manpower study would need to be conducted in order to determine the cost per man hour is needed for training individuals as well as man power analysis on the implementation of the ES-520 in a tactical environment. However, the ES-520 is government contracted and can be commercially bought in the range of \$3,900 and \$4,200, depending on what version is desired.

Finally, the last consideration is strategic and can be answered by the following questions:

1. How satisfied the users are with the current systems?
2. Will the systems be used when installed?

Strategically, will the users be satisfied with the ES-520? Yes, COASTS is an ongoing coalition effort and any technology that can give a tactical advantage would surely satisfy the customer. Moreover, the ES-520 is currently being used in tactical situations. Therefore, it is strategically feasible.

C. SUSTAINABILITY OF THE ES-520

Technological sustainability refers to 1) scalability, and 2) conformity to technology that will be likely to proliferate. Technological sustainability measures how well the implemented wireless technology fits with its environment. In this case, conformity with the 802.11 standards and scalability of the ES-520 network will serve as key indicators [16].

Scalability is the ability of a COTS product to continue to function well when it (or its context) is changed in size or volume in order to meet a user need. Typically, the rescaling is to a larger size or volume. The rescaling can be of the product itself (for example, a line of computer systems of different sizes in terms of storage or new firmware or in the scalable object's movement to a new context (for example, a new operating system). Additionally, it is the ability not only to function well in the rescaled situation, but also to actually take full advantage of it. For example, an application program would be scalable if it could be moved from a smaller to a larger operating system and take full advantage of the larger operating system in terms of performance and the larger number of users that could be handled. In the case of the ES-520, the scalability is based on supportability and performance in the military environment.

When considering the ES-520 for supportability, the following questions arise:

1. What is the maintenance philosophy? Standard or 2M?

2. What is the repair philosophy? Depot Level or Intermediate Level?
Replace or throwaway?
3. If the ES-520 is repaired, then by whom?
4. Who will develop and maintain repair documentation, (Tech
Manuals)
5. What provisions will be made to provide adequate spares?
6. How long will the hardware and or software be supported in the
field?
7. What will drive redesign[16]?

As of now, since Fortress Technologies is a partner in COASTS, some of the answers to the above questions can be would be taken care of by the vendor representative on site. Therefore, maintenance and repair are done by the technician and if the ES-520 needs new firmware or is completely inoperable, it is sent back to Fortress Technologies for repair or replacement.

Regarding performance in a military environment, most COTS vendors do not have experience providing military equipment, or have access to feedback on their equipment's performance in a military environment. At best, they may only see the returned units for repair. Without field usage data (operating time), the COTS vendors cannot measure field reliability. When very little design, test, process, for field performance information is available, the only way to evaluate COTS is to test it. In the case of the ES-520, performance testing has been conducted with the help of the vendor. This thesis, among others, provides the feedback needed to improve the ES-520.

D. ADVANTAGES AND DISADVANTAGES OF THE ES-520

In general, the application of any technology to any problem will have advantages and disadvantages. This holds true for the case of the application of COTS communications technology to military applications. COTS communications technologies and techniques provide both advantages and disadvantages to the military domain. These advantages and disadvantages must be assessed and will generally be

application-specific. Determining the applicability of COTS communications technology to a military application is a complex problem; strong wide-sweeping statements regarding the benefits and drawbacks of COTS are generally over-simplifications that do not exercise a full understanding of the complex problem. It is always important to consider the commercial goals of COTS technologies to ensure that those technologies are not misused within the military domain. Concerning the ES-520, the following sections will discuss advantages and disadvantages as it applies to the military domain.

1. Advantages

There are many potential benefits associated with the use of COTS communications technologies within military communications systems. These benefits include, but are not limited to:

1. Lower acquisition and maintenance cost
2. More robust logistical and support structure
3. Increased flexibility for future technology insertion
4. Improved ease-of-use
5. Faster acquisition cycle time
6. Improved interoperability
7. Wider selection of products/vendors [17]

These benefits are summarized in Table 9.

Advantage	Overview of Advantage
Lower Acquisition and Maintenance cost	The commercial domain can obviously achieve a much greater economy of scale than their more specialized DoD counterparts can. Many mechanisms within the commercial domain enable a more affordable solution. These mechanisms include the demand of consumer needs, the competition of the open market, and the desire to minimize product costs to maximize profit margin. This is an obvious advantage; COTS technologies and techniques can indeed lower the cost of military communications systems.

More robust logistical and support structure	The employment of COTS equipment leads to an obvious improvement in the logistical and support structure associated with that equipment. The ability to replenish equipment from commercial vendors creates a very responsive support structure. These devices are also based on open standards, which ease the need for highly specialized support staff.
Increased flexibility for Future Technology Insertion (FTI)	The open nature of standards-based communications technologies leads to an improvement in FTI. Standards can be modified and translated into commercial products much faster than within the often-proprietary military domain.
Ease-of-use	More importantly, COTS products bring a simplicity and ease-of-use that has never earnestly existed prior within the military domain. When COTS technologies and products are employed, Warfighters are now using the same devices that many of them use in their personal lives. The result is a level of familiarity and expertise that is rarely achieved with proprietary military communications solutions.
Faster acquisition	Military communications solutions are often characterized by long design cycles. COTS technologies tend to exhibit much shorter design cycles and more frequent technology updates, keeping users closer to the state-of-the-art than military users.
Improved interoperability	A significant employment of COTS technologies will provide improved interoperability as all of the next-generation systems are based upon the same standardized technologies, providing a common technological framework within which to interoperate.

Table 9. Advantages of COTS Communications Technologies (From: [17].)

Based on the suggestions on how to rate COTS advantages, the ES-520 fully meets all criteria. The maintenance costs of the ES-520 are low, it has the ability to be upgraded with firmware, as well as, hardware, and the vendor is part of the COASTS program, and therefore there is robust logistical support. Moreover, as the 802.11 technology changes the radios within the unit can be changed to support improved interoperability.

2. Disadvantages

There are also many potential drawbacks associated with the use of COTS communications technologies within military communications systems. These drawbacks include, but are not limited to:

1. Contradictions to future Warfighting concepts
2. Degraded security
3. Limited support of network mobility
4. Lack of scalability
5. QoS limitations
6. Shortened acquisition cycle
7. Wireless "last-mile" problem
8. Military environments [17]

These potential drawbacks are summarized in Table 10. Once again, wide-sweeping statements of benefits of drawbacks of COTS are generally oversimplifications, and the exact drawbacks of a COTS-based solution will be application specific.

Advantage	Overview of Disadvantage
Contradiction of future Warfighting concepts	The issue at hand is that the COTS technologies and products that our fighting forces become dependent on are also available to any potential adversary. As a result, any potential adversary could effectively possess the same communications capability, as well as nearly identical logistical and support structure capability. This shifts the focus of a military operation toward who can "outspend" their adversary to replenish COTS equipment, which is more characteristic of the attrition-based Warfighting paradigm. Indeed, any potential adversary can rely on the same COTS that our fighting forces rely on. This becomes an issue in the NCW paradigm of autonomous fire control missions where it is key that the network be as responsive and effective as possible. In the NCW paradigm, the adversary may also be focused on obtaining information superiority, and may rely on NCW-enabled concepts such as autonomous fire control missions. In this case, the key metric for success is being capable of delivering the required information faster and more reliably than the adversary delivers. If COTS is the delivery mechanism, it is unclear if that is guaranteed to be the case.
Degraded security	The commercial world will never likely fully meet the needs of the military user in a few key technological areas. This is because the core business area of the commercial world will always remain the commercial user; the military user consumer base is inherently smaller than the commercial consumer base. As a result, the needs of the commercial consumer base will likely always remain the top priority,

	<p>such as support of true ad-hoc networking, end-to-end QoS support, and security in general. Security needs within military communications are more stringent than in the civilian world. Furthermore, there are dimensions of military security that have no counterpart within the civilian domain such as covertness. Commercial communication technologies are not typically designed to withstand intentional interference. There are known issues regarding intentional and unintentional interference with the IEEE 802.11b, 802.11a, 802.11g, and Bluetooth commercial technologies.</p>
Limited support of network mobility	<p>Many COTS technologies and techniques do not support network mobility to the degree required by the military. Certain commercial WAN standards do not support mobility from a physical layer or network layer perspective. For example, previous analysis and lab experiments have indicated that the association process of the IEEE 802.11 WLAN standards does not accommodate the Doppler frequency effects of very fast-moving platforms, even though the standard itself indicates that these frequency shifts should be tolerable. Most Internet protocols are designed to operate over the wired Internet environment, and are not intended to accommodate a dynamically changing wireless network. There are current efforts within the IETF to create new protocols that can accommodate the mobile Internet paradigm, but are still predicated upon some type of infrastructure; infrastructure will not always exist for the deployed military network.</p>
QoS limitations	<p>Military QoS is very different from commercial QoS. Military QoS is both mission and application driven, independent of the environment. The military ideally requires stringent QoS capability that can be prioritized by both mission and application and is flexible. Commercial QoS technologies developed within the IETF are predicated on benign channel conditions and perform better when the network is highly over-provisioned. In the military domain, this is rarely the case, particularly for the wireless networks supporting the end users. Additionally, in the commercial domain networks provide QoS to one another based upon pre-negotiated Service Level Agreements (SLA). These SLAs usually consists of soft performance guarantees based upon negotiated agreements of understanding. There are a couple of issues that arise when applying this type of QoS architecture to the military domain: 1) the validity of an SLA construct, and 2) the need for end-to-end hard (or harder) guarantees. The key penalty if a commercial network does not meet the promises within the SLA is monetary. It is unclear what corresponding penalty metric would be employed within the military domain. Clearly, hard guarantees cannot be provided when the end-user is attached to a wireless network. Nevertheless, the Warfighter still requires much harder performance guarantees than is typically provided in the commercial world. In fact, the entire concept of NCW is predicated on the network being highly reliable. This reliability includes</p>

	the network's ability to provide its requested QoS regardless of the changing network.
Shortened acquisition cycle	The shortened acquisition cycle introduced by COTS technologies was previously mentioned as an advantage of COTS. This attribute can also be a potential disadvantage. Indeed, certain standards organizations are predicated on pushing experimental technologies to market in order to spawn implementations and feedback data to refine the technology. Historically, this has not been the approach of the military community. The military community has previously been characterized by a long acquisition cycle in order to fully study a problem and deploy a fully capable solution. There is the potential that inadequate technology could be fielded if the "rush-to-market" commercial approach is employed. The military domain requires a well-researched solution that has been thoroughly evaluated prior to deployment; anything less would be irresponsible and operationally unacceptable, as this would needlessly place Warfighters at risk. The characteristic of FTI is much more important than acquisition cycle time. If a deployed communications solution possesses a high degree of FTI friendliness, than future solutions can be fielded incrementally, which inherently leads to shorter acquisition times.
Military environments	Lastly, the military environment itself can mitigate the effectiveness of COTS solutions if COTS is taken to mean off-the-shelf devices deployed to field. COTS devices have rarely been designed to function within the environments required by the military user, such as rain, snow, mud, dust, dirt, and sand. These devices also have not been designed to tolerate the types of abuse they are going to withstand within the military application, such as exposure to extreme heat and cold, shock, and rough handling.

Table 10. Disadvantages of COTS Communications Technologies in Military Applications (From: [17].)

Contradiction of future warfighting concepts seems it may be a problem. However, this may be the case with any COTS technology used by the military. Only the contractors know if this technology is available to the adversary. Therefore, the making an assumption whether the ES-520 meets this disadvantages would not be reasonable. The ES-520 does not fall under any of the remaining listed disadvantages.

E. SUMMARY

This chapter offered guidance in the selection of the ES-520 based on feasibility, sustainability, and technical advantages and disadvantages. The next chapter summarizes the research

VI. CONCLUSION

A. RESEARCH SUMMARY

Chapter II provides a discussion of military requirements for secure wireless communications, the COASTS 2007 international field experimentation program, and the ES-520 capabilities.

Chapter III provides an overview of previous research that evaluated military necessity versus the current state-of-the-art in 802.11 devices.

Chapter IV discusses the methodology used in the research of the ES-520 as well as provides an analysis of the results with regard to the MOEs and MOPs to address the capabilities and limitations of the equipment.

Chapter V provides a review of the feasibility, sustainability, and technical advantages/disadvantages of the ES-520.

Chapter VI recommends future implementation and experimentation in the COASTS environment as it pertains to high throughput tactical wireless networking regarding COTS 802.11 technology.

B. OBSERVATIONS

The ES-520 was tested for maximum distance and LOS, under the premise that a military unit would set up the non-root node in the field to communicate with Command and Control. MOE and MOP were analyzed using the appropriate measures and IxChariot. During both field experiments the ES-520 experimentation phases of the effectively transmitted data, as simulated by the IxChariot network evaluation suite, across both the root node and non-root node. As previously described, the IxChariot network evaluation suite mimicked the transfer of text, audio, and video data using the throughput.scr to analyze the network's throughput, transaction rate, and response time, as shown in the previous section. The evaluation was conducted in both a local area network and wide area network. Therefore, the ES-520 is effective in both situations.

Compliance with standards allows the ES-520 to operate in conjunction with other compliant networks assuming employment of the proper routing and configuration. This allows the ES-520 to network across most previously established infrastructures or to operate without any previous network infrastructure. Concerning physical characteristics, the ES-520 is portable, but only to the extent of the nearest power supply. The lack of an internal battery (or other self-sufficient power supply) limits the device's usefulness in severe locations. There were no problems operating in both of the field experiment locations once a useful power supply was found to support the required 48 VDC to operate the ES-520. The testing conducted was in California, results might vary in other operating environments due to thermal overload or signal interference. Additionally, because of the ES-520's weatherizing kit, the device is expected to operate tolerably; however, the equipment was not tested in other environments.

The ES-520 router is somewhat user friendly. The level of the user's experience to deploy the network must be at a level above an intermediate level user. Although the ES-520 has a software setup wizard, which allows for connection, a much greater knowledge of network configuration is necessary to deploy the ES-520 with existing infrastructure. This is especially true when one is attempting to troubleshoot and to repair the network. Special knowledge of the network architecture, IP addressing scheme and router configuration are particularly important.

The ES-520 is intuitive to operate and configure, the equipment is a complete implementation of the emerging IEEE 802.11 standard. Therefore, it is an appropriate solution for the COASTS environment. The complete ES-520 kit is readily deployable. Particularly, this equipment is ruggedized and simplified for an expeditious environment. The ES-520 should include the internal batteries or adequate power supply to support the power requirement. Because of this research, the ES-520 promises to provide high throughput but not in the case where a military unit can quickly set up and receive data. It seems it would be suited for a multiple hop network where technicians have more time to set up to receive optimum throughput. Additionally, if the ES-520 were used over greater distances one might contemplate the use of directional antennas.

C. LESSONS LEARNED

Several important lessons were learned during the experimentation process. Many of the lessons learned were the result of actions or difficulties that could not be controlled. Other lessons learned were oversights or challenges that might have been avoidable given additional time and resources.

The first lesson learned during the testing and scenario demonstration processes was the importance and difficulty of power management. The challenge of power management was discussed previously regarding wireless sensor networks. The challenge became evident when deploying the ES-520. Initially, 48 VDC was provided by batteries put in series. This was not a viable source of power due to logistics. Once adequate power supplies were found testing went smoothly.

The second lesson learned is based on the research question: What is the network reliability of operating the Fortress Secure Wireless Access Bridge (ES-520) in different environments? Due to time and location selection, this question could not be answered. The ES-520 was only tested in California with similar environments. Therefore, if proper planning had been completed this part of the research would have been conducted.

The third lesson learned is that integrating COTS technologies for military applications can be very difficult. The entire COASTS network consisted of commercially available technologies. As a result, integration issues often arose. In addition, the manufacturer's support significantly influences the success of integrating the technology. For example, successful completion of this research was highly dependable on vendor technician presence. Fortunately, these difficulties helped to highlight the importance of cooperation between the user and manufacturer for applying the ES-520 to the research proposed.

D. AVENUES FOR FUTURE RESEARCH

After extensive research of the ES-520, other areas are suitable for future research. The avenues for future research can be divided into the broad mobility, air, and sea categories.

First, in regards to mobility, as stated in this research, the military is inherently mobile. Therefore, in future research the ES-520 should be testing on moving platforms. One foreseeable problem in the study of mobility would be Doppler Effect. Doppler Effect is the change in frequency and wavelength of a wave as perceived by an observer moving relative to the source of the waves. Doppler Effect in wireless communications is generated, if a transmitter or receiver is moving the frequency of the received signal is lower than the one sent from the transmitter; otherwise, the frequency is increased. When research is conducted in mobility careful consideration must be made regarding Doppler Effect and possibly access the acceptable risks to leverage the full capacity of the ES-520. Secondly, in regards to air, can the ES-520 support air platforms and up to what speeds? Air platforms would greatly increase the range of the nodes created in an ad hoc architecture. Air platforms would enable over the horizon communications for military units. Again, one must consider Doppler Effect. Additionally, in a tactical environment air platforms such as balloons may not be feasible because of limited defense.

Lastly, in regards to sea, the same questions arise. What speeds can be supported? What affect will salt water have on the system and how much of a difference does the ES-520 signals propagate at sea? 802.11 propagate over land and water differently. The research with the ES-520 could validate whether it is a viable option for sea platforms.

APPENDIX: ES-520 NETWORK SUPPORTING HARDWARE AND SOFTWARE SPECIFICATIONS

A. INTRODUCTION

This chapter introduces the experimental system and its specifications – the Fortress Technologies Secure Wireless Access Bridge (ES-520). The supporting hardware and software used in this research are also discussed. These include the 3COM switch, West Marine Battery, PowerBright Power Inverter, Garmin Foretrex 201, the “Google Earth” application, Antennas, Laptop computers, and the Test Application, “IxChariot.”

B. FORTRESS TECHNOLOGIES SECURE WIRELESS ACCESS BRIDGE (ES-520)

The Fortress Secure Wireless Access Bridge is an all-in-one network access device. It can serve as a wireless bridge, a WLAN access point, and an eight-port LAN switch, while performing all the functions of a Fortress controller device: encrypting wireless traffic and providing Multi-factor Authentication for devices on the network it protects. Figure 11 illustrates the ES-520. Table 11 and the following sections describe key components and specifications of the ES-520.



Figure 11. Fortress Technologies Secure Wireless Access Bridge (ES-520) (From: [18].)

FEATURES AND PERFORMANCE	
Range	Tested up to 32 miles (directional antenna) Tested up to 7 miles (omnidirectional antenna)
Performance	Up to 100 secure clients
Encryption	AES-128, 192, 256 WPA2 (802.11i) Suite B software module (available Q1 2007)
Authentication	Internal or external RADIUS, PKI/CAC User and device
Intrusion Detection	Wireless Intrusion Detection module (available Q1 2007)
Management	Secure browser-based GUI, CLI or SNMP
SSID Support	Up to 4 SSIDs
HARDWARE	
Enclosure	Rugged .125" aluminum NEMA 4
Mounting	Mast mounting kit and weatherizing kit included
Dimensions	2.7"H x 8.8"W x 6.7"D (6.9cm x 22.4cm x 17.1cm)
Weight	3.46 lbs. (1.57 kg)
Connections	Eight RJ-45 10/100 LAN ports with auto-MDIX One RJ-45 10/100 WAN port with PoE receiver One RJ-45 serial console port Two USB ports for future functionality
Radios	One 200 mW 802.11a/b/g radio (maximum transmit power 23dBm) One 400 mW 802.11a radio (maximum transmit power 26dBm)
Antenna Support	2 N-style external antenna connectors (female)
Radio Modes of Operation	Wireless access point or bridge
Power Supply	External AC-DC power adapter (48V), or PoE (PoE injector included) Polarity protection
Power Draw	13W maximum
Port LEDs	Link, activity, status, PoE
Radio LED	Strength and association
Warranty	Includes 1 year of Maintenance and Support
ENVIRONMENTAL	
Cooling	Convection (no fans)
Operating Temperature	-10 ~ 50°C
Humidity	5 ~ 95%

FEATURES AND PERFORMANCE	
Weather Resistance	Water-resistant front panel cover plate included IP56 NEMA 4 Lightning arrestor
Vibration, Bounce & Shock	MIL-STD 810F
CERTIFICATIONS	
Safety & Emissions	CE, FCC, UL 60950-1, IEC 60529 (CB Test)
NIST	FIPS 140-2 level 2 submitted
Common Criteria	EAL 3 submitted

Table 11. ES-520 Specifications (From: [18].)

The ES-520 has two radios capable of the following:

1. Radio 1 is a tri-band 802.11a/b/g radio that can be configured to use either the 802.11b/g band or the 802.11a band. It can function as a wireless access point (AP), providing secure WLAN connectivity to wireless devices within range, or as a wireless bridge in a point-to-point or point-to-multipoint network.
2. Radio 2 is fixed on the 802.11a band. As the higher powered of the two radios, it would normally be the first choice for the bridging function in a mixed AP/wireless bridge deployment, but it can equally function as an 802.11a AP [18].

Additionally, the ES-520 has eight RJ-45 10/100 Mbps Auto-MDIX Ethernet ports (labeled 1-8) are connectors for the Bridge's internal LAN switch.

1. Components

The ES-520 comes with several components when purchased. The package includes:

1. Fortress Secure Wireless Access Bridge
2. one universal AC-to-48V DC power adapter (Figure 12.)
3. AC power cord (Figure 12.)

4. one EBU-101-01 PoE adapter (Figure 13.)
5. one RJ-45-to-DB9 adapter (for use with a standard, straight-through CAT5 assembly) (Figure 14.)
6. ES-520 Weatherizing Kit, including: (Figure 15.)
 - a. one front-panel cover plate
 - b. one RJ-45 connector boot assembly (six pieces)
 - a. one antenna port cap
7. ES-520 Mast-Mounting Kit, including: (Figure 16.)
 - b. one mast mounting bracket
 - c. two 4" long, fully threaded 1/4-20 hex bolts
 - d. two 1/4" split lock washers [18]



Figure 12. Universal AC-to-48V DC Power Adapter and AC Power Cord



Figure 13. EBU-101-01 PoE Adapter (From: [19].)



Figure 14. RJ-45-to-DB9 Adapter



Figure 15. ES-520 Weatherizing Kit

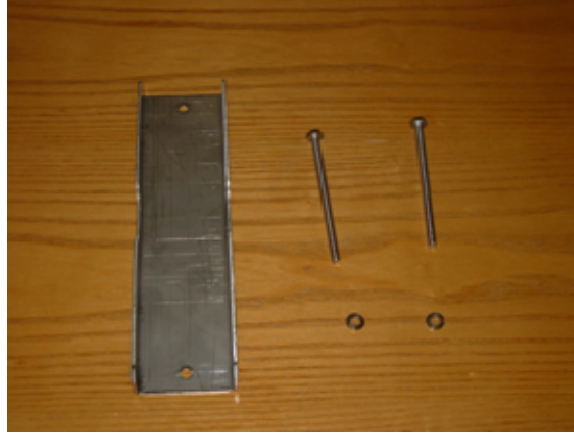


Figure 16. ES-520 Mast-Mounting Kit

2. Functional Description

a. ES-520

Figure 17 illustrates the front panel of the ES-520.

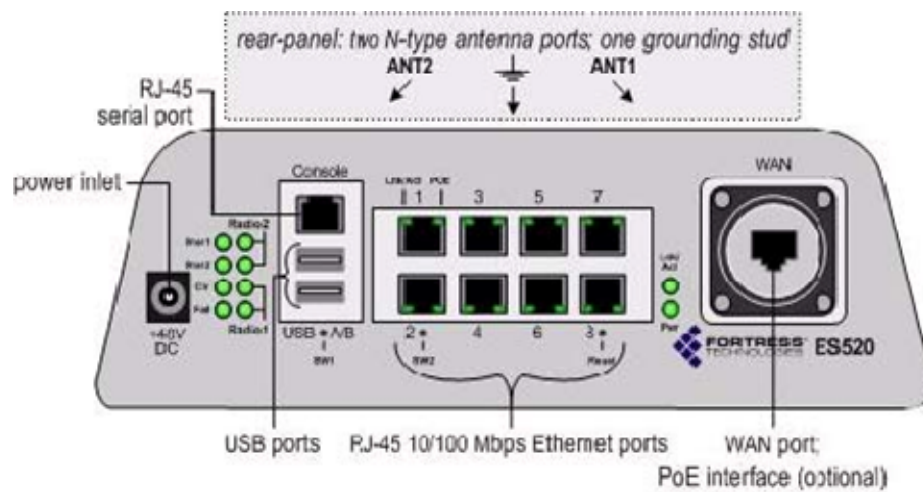


Figure 17. ES-520 Port Locations (From: [18].)

b. EBU-101-01 PoE Adapter

The EBU-101-01 PoE adapter included with the ES-520 is a Senao product capable of providing Power over Ethernet (PoE). It has two Ethernet ports – one for data input and one for power and data out. Tables 12 and 13 provide specifications for the EBU-101-01 PoE Adapter.

Ethernet Connector	RJ-45
Ethernet Data Rate	10/100 Mbps
DC-Input	48V - Applied from external switching adapter
DC-Output	Pins 4,5 (up to +48V), Pins 7,8 (GND)
Green LED	Power Indicator
Operating Temp	-10C to +70C
Humidity (non-condensing)	Up to 95%
Dimensions	2.1 x 1.7 x 1.0in (54 x 42 x 26 mm)

Table 12. EBU-101-01 PoE Specifications (From: [19].)

Pin	Input / SK1	Output / SK2
1	Tx (+)	Tx (+)
2	Tx (-)	Tx (-)
3	Rx (+)	Rx (+)
4	N.C.	+V
5	N.C.	+V
6	Rx (-)	Rx (-)
7	GND	GND
8	GND	GND

Table 13. EBU-101-01 PoE Pin Designators (From: [19].)

c. RJ-45-to-DB9 Adapter

A RJ-45-to-DB9 adapter (included with each Bridge) is required in order to connect the Bridge's Console port to a DB9 terminal connection [18].

Figure 18 shows the pin numbers for the two connectors. With the RJ-45 connector facing you and oriented with the tab receptacle up, pins are numbered from left

to right, as shown. With the DB9 connector facing you and oriented with the wide side up, pins are numbered from right to left, top to bottom.

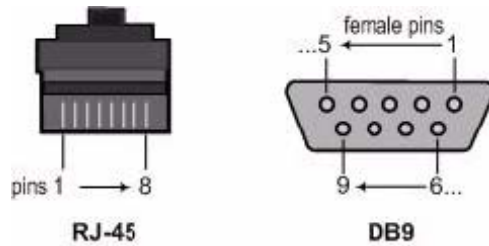


Figure 18. RJ-45 and D89 Pin Numbering (From: [18].)

d. ES-520 Weatherizing Kit

The ES-520 has a UL (NEMA) 3/3S/4 rain tight rating. The Front-panel Cover Plate of the ES-520 Weatherizing Kit provides additional protection to the unit. Additionally, a WAN-port RJ-45 connector boot assembly and antenna cap is included. When the Weatherizing Kit is installed, the only available connections to the Bridge are the front-panel WAN port and the rear-panel antenna ports [18]. Figures 19 and 20 illustrate the proper use of the Weatherizing components.

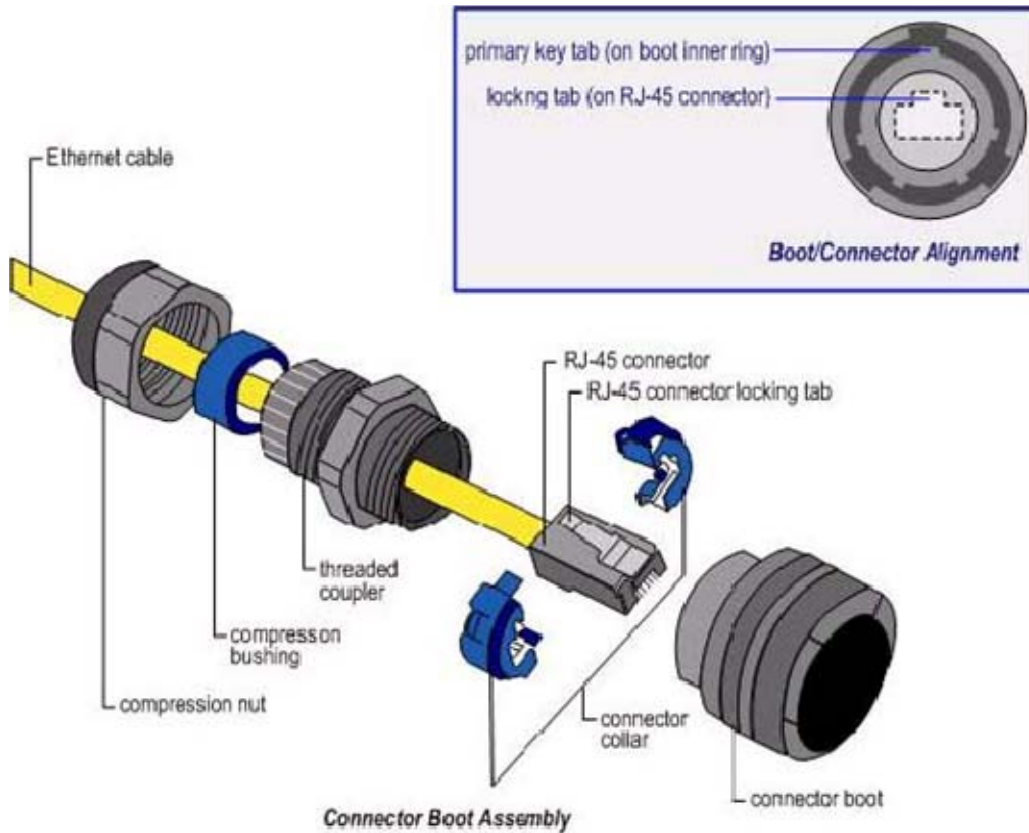


Figure 19. Weatherizing the RJ-45 Connector Boot Assembly (From: [18].)

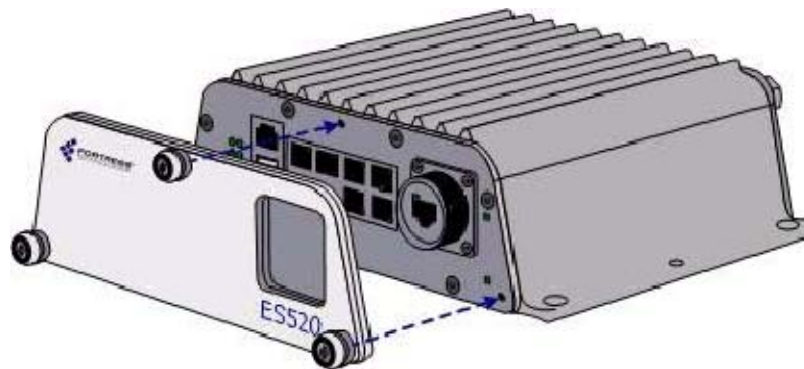


Figure 20. Attaching the Front-Panel Cover (From: [18].)

e. ES-520 Mast-Mounting Kit

Included with the ES-520 is mast-mount equipment. When installing the ES-520 outdoors, Fortress suggests the use of Mast-Mounting Kit. Before installing the Bridge in a hard-to-reach, outdoor location, Fortress recommends connecting and pre-configuring the Bridge. The Mast-Mounting Kit accommodates masts from 1.5" to 3" in diameter. Figure 21 illustrates how to install an ES-520 to a mast.

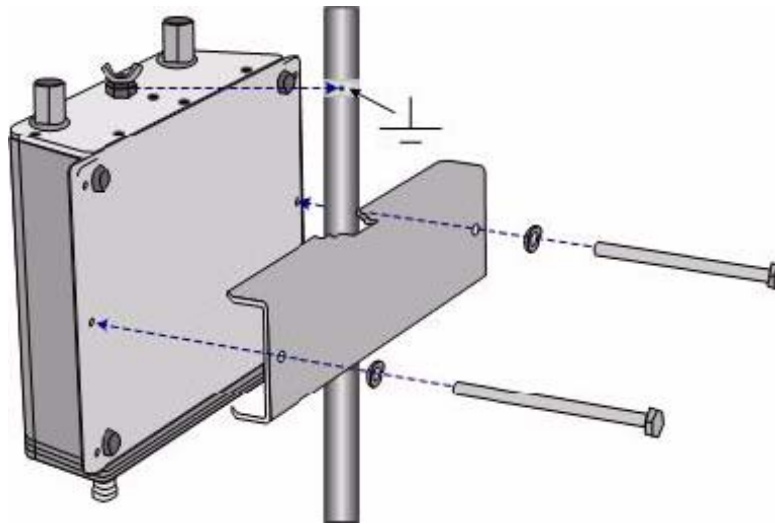


Figure 21. Attaching the Mast-Mounting Bracket and Grounding Stud (From: [18].)

C. 3COM SWITCH

Incorporated into the experiment of the ES-520 was the switch that was part of the TOC. The TOC uses the 3Com Baseline Switch 2824-SFP Plus to create a network.

The 3Com Baseline Switch 2824-SFP Plus is a versatile, easy-to-use configurable Switch. It is ideal for high-speed performance of 10/100/1000 switching with the added functionality of Gigabit links. The Switch has 16 24 shielded RJ-45, 10/100/1000 Mbps auto-negotiating ports and four Small Form Factor Pluggable (SFP) transceiver slots on the front panel for easy, flexible connection to fiber-based Gigabit media [20]. Figure 22 shows a 3Com Baseline Switch at the TOC of COASTS Fort Hunter Liggett experiment.



Figure 22. Photo of 3COM Baseline Switch 2824-SFP Plus

D. WEST MARINE SEAGEL MARINE GEL BATTERY

The non-root ES-520 required power other than the power provided in the Tactical Operations Center (TOC). Power supplied to the non-root ES-520 was provided by the West Marine SeaGel Battery through the PowerBright Inverter. The Marine Gel Battery provided 12V DC. Figure 23 is a photo of the battery. Listed below are some characteristics of the battery:

1. Self-discharge rate allows the batteries to sit without significant power loss
 2. Even when left discharged for 30 days will come back to 100% capacity
 3. Extra-thick lead calcium plates will not sulfate
 4. Capable of over 500 full discharges in temps from -22° to + 122°
 5. These batteries charge at lower voltages than Deep Cycle or AMA
- [21]



Figure 23. Photo of Marine Gel Battery

E. POWERBRIGHT POWER INVERTER

Another item required for the non-root ES-520 was a power inverter. The power inverter transformed the Direct Current (DC) voltage from the marine battery to a usable Alternating Current (AC) Voltage. Specifically, the Power Bright 1100 was used for the experiment. Figure 24 illustrates the power inverter and Table 14 displays its specifications.



Figure 24. PowerBright 1100 Watt 12 Volt DC-to-AC Power Inverter (From: [22].)

SPECIFICATIONS	
Continued Power	1100W
Peak Load Power Rate	< 2200W
Overload Output Power	1150-1300W
No Load Current Draw	< 0.9A
Input DC Voltage Range	11-15V
Output Voltage Range	117 +/- 10%
Output Frequency Range	60 +/- 3Hz
Max Outer Temperature	< 65 C
Max Power Efficiency	> 80%
High Voltage Cut Off Level	16.5 +/- 1V
Low Voltage Alarm Level	10.5 +/- 0.5V
Low Voltage Cut Off Level	10 +/- 0.5V
Short Protect	Yes
Overload Protect	Yes
Dimension (LxWxH) mm	259x147x69
Weight	1.9 Kg
Standard Test Voltage Input	DC 12V

Table 14. PowerBright 1100 Watt 12 Volt DC-to-AC Power Inverter Specifications (From: [22].)

F. GARMIN FORETREX 201

In this research, there was a requirement to determine the distance separation between the root ES-520 and the non-root ES-520. The Garmin Foretrex 201 was used in this research. Together with the “Google Earth” application (discussed in the next section), the distance separation is calculated. Figure 25 shows the Garmin Foretrex 201. Table 15 displays features of the Garmin Foretrex 201.



Figure 25. Garmin Foretrex 201 (From: [23].)

GPS accuracy	15 meters or less in normal GPS mode, 3 meters or less when WAAS-enabled
Racing timers	Configurable start sequence, alert tones and large-number digital readout
Trip computer	Trip distance, trip timer, plus essential navigation data
Waterproof	IEC 60529 IPX-7 standards (submersible in one meter of water for up to 30 minutes)
Waypoints and routes	500 waypoints with graphic identification; 20 reversible routes
Track log	10,000 trackpoints, TracBack technology and 10 saved tracks
Display	100x60-pixel monochrome display with backlighting (display size: 36mmx23mm)
Battery life	15 hours (typical use), rechargeable lithium battery
Lightweight design	2.75 oz.
Unit dimensions	3.3" W x 1.7" H x 0.6" D (8.38 cm x 4.32 cm x 1.52 cm)

Table 15. Garmin Foretrex 201 Features (From: [23].)

G. GOOGLE EARTH

The Google earth application provides a detailed three-dimensional terrain map of the Earth. By entering data from the Garmin Foretrex 201, the distance separation between points can be calculated. Figure 26 shows a screen capture of the Google Earth application, where the distance separation between two test points is displayed.



Figure 26. Screen Capture of Google Earth Application

H. ANTENNAS

Each Test run used particular antennas to see if better results could be received. The antennas used are illustrated in Figures 27 through 31 and depicted described in Tables 16 through 20.

1. Pacific Wireless 2.4GHz 7dBi Antenna



Figure 27. Photo of Pacific Wireless 2.4 GHZ 7dBi Antenna (From: [24].)

The 2.4GHz 7dBi Pacific Wireless Antenna depicted in Figure 27 is described in Table 16.

Parameter	Min	Typ	Max	Units
Frequency Range	2400		2485	MHz
Input Return Loss (S_{11})		-14		dB
VSWR		1.5:1		
Impedance		50		OHM
Input Power			100	W
Pole Diameter (OD)	1 25		2 50	inch mm
Operating Temperature	-40		+70	Deg C
2400 – 2485 MHz	OD24-7D5			
Gain	7dBI			
Vertical Beam Width	18 Degrees			
Electrical Downtilt	5 Degrees			
Rated Wind Velocity	125mph (56m/sec)			

Weight	1.1 Lbs (0.5Kg)
Dimension (L +/-1.0")	21" (54cm)
Diameter Approx.	0.6" (15mm)

Table 16. Technical Specification of 2.4GHz 7dBi Pacific Wireless Antenna (From: [24].)

2. Superpass 5.8GHz 8dBi Antenna



Figure 28. Photo of 5.8GHz 8dBi Superpass Antenna (From: Ref. [25].)

17. The 5.8GHz 8dBi Superpass Antenna depicted in Figure 28 is described in Table

ITEM	DESCRIPTION
Frequency Range	5250 – 5900 MHz
Impedance	50 W
VSWR (or Return Loss)	$\leq 1.5:1$ (or $\geq 14\text{dB}$)
Gain	8dBi
Polarization	Vertical, Linear
3dB Horizontal Beamwidth	360°
3dB Vertical Beamwidth	18°
Max. Power Input	20W
Connector	N female
Appearance	See attached drawing
Size	10" x 1"
Housing Material	Fiber-Glass
Radome Material	ASA with UV Protection
Radome Color	Gray or White
Case Design	Water Resistance
Weight	0.5 Lb
Wind Loading (Frontal)	$\geq 10\text{Kg}$

Temperature Range	-45 to +75 ° C
Storage Temperature	-30 to +75 ° C
Sensing Resistor or DC-Ground	DC-Grounded
Life Expectancy	20 years

Table 17. Technical Specifications of 5.8GHz 8dBi Superpass Antenna (After: [25].)

3. Hyperlink 5.8GHz 8dBi Antenna



Figure 29. Photo of Hyperlink 5.8GHz 8dBi Antenna (From: [26].)

18. The 5.8GHz 8dBi Hyperlink Antenna depicted in Figure 29 is described in Table

Frequency	5725-5850 MHz
Gain	8 dBi
Polarization	Vertical
Horizontal Beam Width	360°
Vertical Beam Width	16°
Impedance	50 Ohm
Max. Input Power	100 Watts
VSWR	< 1.5:1 avg.
Lightning Protection	DC Short

Connector	N Female
Weight	.44 lbs. (0.2 kg)
Dimensions	.78" (20 mm) Dia. x 13.7" (350 mm)
Radome Material	Gray Fiberglass
Operating Temperature	-40° C to 85° C
RoHS Compliant	Yes
Mounting	2" (50.8 mm) dia. mast max.

Table 18. Technical Specifications of Hyperlink 5.8GHz 8dBi Antenna (After: [26].)

4. TerraWave 5.8GHz 10dbi Antenna



Figure 30. Photo of TerraWave 5.8GHz 10dBi Antenna (From: Ref. [27].)

The 5.8GHz 10dBi TerraWave Antenna depicted in Figure 30 is described in Table 19.

Specifications	
Model	T58100O10006
Frequency Range	5725 - 5850 MHz
Bandwidth	125 MHz

Gain	10 dBi
Vertical Beamwidth	10°
VSWR	-/ = 1.5
Impedance	50 Ohms
Polarization	Vertical
Maximum Power	100 Watts
Connector	N-Style Jack
Height	16.9"
Weight	0.5 lbs
Horizontal Beamwidth	360°
Rated Wind Velocity	135 mph
Operating Temperature	-22°F - 158°F

Table 19. Technical Specifications of TerraWave 5.8GHz 10dBi Antenna (From: [27].)

5. Hyperlink 5.8GHz 12dBi Antenna



Figure 31. Photo of Hyperlink 5.8GHz 12dBi Antenna (From: [28].)

The 5.8GHz 12dBi Hyperlink Antenna depicted in Figure 31 is described in Table 20.

Frequency	5725-5850 MHz
Gain	12 dBi
Polarization	Vertical
Vertical Beam Width	6°
Horizontal Beam Width	360°

Impedance	50 Ohm
Max. Input Power	150 Watts
Lightning Protection	DC Short
Weight	1.5 lbs (0.7kg)
Length	29.4 in. (0.7m)
Base Diameter	2.28 in. (57.9mm)
Radome Diameter	2.04 in. (51.8mm)
Radome Material	Fiberglass
Mounting	1.4 in. (35 mm) to 2.0 in. (50 mm) dia mast
Rated Wind Velocity	137 MPH/S (220Km/S)
Operating Temperature	-40° C to 85° C
Connector	Integral N-Female
RoHS Compliant	Yes

Table 20. Technical Specifications of Hyperlink 5.8GHz 12dBi Antenna (From: [28].)

I. IXCHARIOT

IxChariot version 6.40 by IXIA was the software tool used to measure the system performance under throughout each experiment. IxChariot was created by Ixia, a publicly held company specializing in network performance testing tools. IxChariot was chosen mainly for its ease of use and reputation as being one of the best software tools available for monitoring and testing network throughput. One Dell Laptop was loaded with the IxChariot console as shown in Figure 32.

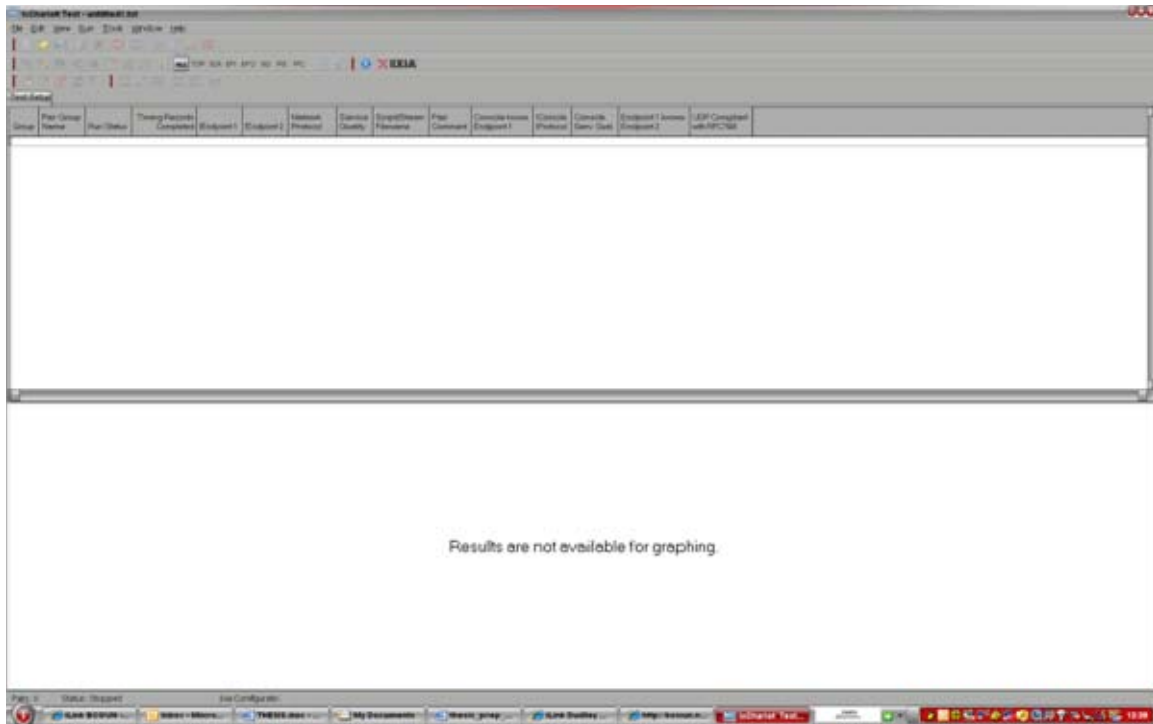


Figure 32. Screen Capture IxChariot Console

J. LAPTOP COMPUTERS

As mentioned in the previous section, one dell laptop was loaded with the IxChariot console. Two additional laptop computers were needed for the experimentation of the ES-520. One computer connected to the Root node and one to the non-root node. For the experiment, each had to be loaded with an endpoint application from IxChariot. With the endpoint running in the background, IxChariot was able to complete analysis of data sent. Additionally, the Root node computer and the IxChariot computers were routed through the 3COM switch. For successful operation of each test, the computers did not run a firewall, anti-virus software, or screensavers. Table 21 presents the specifications of the three laptops that were used for the purposes of this research.

Characteristics	IxChariot Laptop	Root node Laptop	Non-root node Laptop
Type	Dell Latitude D510	Dell Latitude D610	Dell Inspiron E1705
Computer Processor	Intel Pentium M 1.86 GHz	Intel Pentium M 1.60 GHz	Intel Centrino Duo 1.828 GHz each
Operating System	Windows XP (SP2)	Windows (SP2)	Windows XP (SP2)
RAM	2 GB	512 MB	1 GB
Hard-disk	80 GB	60 GB	80 GB
Display	15", 1024 x 768 (resolution)	14.1", 1024 x 768 (resolution)	17", 1920 x 1200 (resolution)

Table 21. Specifications of the Laptop Computers used in the Experimentation of the ES-520

K. SUMMARY

The chapter presented all equipment use for the experimentation of the ES-520. The next chapter will present the procedures and methodology used in the experimentation of the ES-520.

LIST OF REFERENCES

- [1] Hearst Business Communications, "Secure Communication," http://semiapps.com.cn/print.php?content_id=61221212408902196. Last accessed 5 February 2008.
- [2] James F. Ehlert, "*Cooperative Operations and Applied Science & Technology Studies 2007: Concept of Operations*," 22 February 2007.
- [3] Fortress Technologies, "Fortress Bringing Secure Communications Anywhere at Anytime," <http://www.fortresstech.com/media/Fortress%20Wireless%20Communications%20System.pdf>. Last accessed 5 February 2008.
- [4] Mazda Salmanian, "Military Wireless Network Information Operation Scenarios," Dec 2003 <http://cradpdf.drdc-rddc.gc.ca/PDFS/unc17/p520923.pdf> Last accessed 5 February 2008.
- [5] Pierpaolo Bergamo, et al., "IEEE 802.11 Wireless Network under Aggressive Mobility Scenarios," <http://www.cs.ucla.edu/ST/docs/itc2003.pdf> Last accessed 2 February 2008.
- [6] Zygmunt J Haas; Siamak Tabrizi, "On Some Challenges and Design Choices in AD-HOC Communications," 25 January 2000, Cornell University. <http://stinet.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA428395>. Last accessed 2 February 2008.
- [7] Kiran P Diwakar, "Intelligent Access Point Guaranteeing QoS in 802.11," Kanwal Rekhi School of Information Technology, Indian Institute of Technology, Bombay Mumbai, http://www.it.iitb.ac.in/~kiran/kiran_second_stage_report.pdf Last accessed 2 February 2008.
- [8] John Bellardo; Stefan Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," University of California, <http://users.csc.calpoly.edu/~bellardo/pubs/usenix-sec03-80211dos-color.pdf>. Last accessed 2 February 2008.
- [9] Richard North; Dale Bryan, "*Wireless Networked Radios: Comparison of Military, Commercial, and R&D Protocols*," Second Annual UCSD Conference on Wireless Communications, San Diego, CA February 28 – March 3, 1999, <http://66.102.1.104/scholar?hl=en&lr=&q=cache:TceVIYJMACUJ:www.adiesa.aeema.asn.au/documents/WirelessNetworkedRadios-ComparisonofMilitaryCommericalandRDProtocols.pdf+Robustness+802.11+devices+military>. Last accessed 7 February 2008.

- [10] Roberto Battiti, Thang Le Nhat, and Alessandro Villani, “*Location-Aware Computing: A Neural Network Model For Determining Location in Wireless Lans*” University of Trento, Povo – Trento (Italy), Via Sommarive 14, February 2002. <http://rtm.science.unitn.it/~battiti/archive/blv2002.pdf>. Last accessed 7 February 2008.
- [11] S. Zhao, K. Tepe, I. Seskar, and D. Raychaudhuri, “Routing Protocols for Self-Organizing Hierarchical Ad-Hoc Wireless Networks.” Rutgers University, Piscataway, NJ, <http://www.winlab.rutgers.edu/~sulizhao/isRtHierAdhoc.pdf>, Last accessed 7 February 2008.
- [12] J. Macker and S. Corson, “IETF Mobile Ad hoc Networking Working Group Charter,” www.ietf.org/html.charters/manet-charter.html, Last accessed 9 February 2008.
- [13] Atheros Communications, “Methodology for Testing Wireless LAN Performance with Chariot,” http://atheros.com/pt/whitepapers/Methodology_Testing_WLAN_Chariot.pdf, Last accessed 7 February 2008.
- [14] Damian Pianta, “Measures of Effectiveness (MOE) and Measures of Performance (MOP), The University of Queensland, http://www.catalyst.uq.edu.au/designsurfer/MoE_MoP.pdf, Last accessed 7 February 2008.
- [15] University of Southern California, “Model Rationale,” Center for Systems and Software Engineering. <http://sunset.usc.edu/research/COCOTS/index.html> 10/22/2001, Last accessed 7 February 2008.
- [16] Edward Demko, “Commercial-Off-The Shelf (COTS): A Challenge to Military Equipment Reliability,” Northrop Grumman, Melbourne. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=500634, Last accessed 8 February 2008.
- [17] Jack L. Burbank; William T. Kasch, “*COTS Communications Technologies for DoD Applications: Challenges and Limitations*,” Johns Hopkins University, MILCOM 2004 - 2004 IEEE Military Communications Conference.
- [18] Fortress Technologies, “Fortress Secure Wireless Access Bridge: ES-520 Specifications,” http://www.fortresstech.com/products_services/pdfs/ftprod_ES-520fed.pdf. Last accessed 20 February 2007.
- [19] Moonblink, “Senao Power over Ethernet (PoE) Injector,” http://www.moonblinkwifi.com/pd_senao_poe_injector.cfm, Last accessed 20 February 2007.

- [20] 3Com, “Baseline Switch 2816-SFP/2824-SFP Plus: User Guide,” <http://support.3com.com/infodeli/tools/switches/3C16485/DUA1648-5AAA03.pdf>, Last accessed 22 February 2007.
- [21] West Marine, “SeaGel Gel Batteries,” <http://www.westmarine.com/webapp/wcs/stores/servlet/ProductDisplay?storeId=10001&langId=-1&catalogId=10001&productId=29254>. Last accessed 25 February 2007.
- [22] PowerBright, “PBI1100 Specifications,” http://www.powerbright.com/pdf/pbi1100_spec_sheet.pdf. Last accessed 20 February 2007.
- [23] Garmin, “Foretrex 201,” <http://www.garmin.com/products/foretrex201/>. Last accessed 20 February 2007.
- [24] Pacific Wireless, “2.4 GHz VPOL Omni Antennas,” http://www.pacwireless.com/products/omni_vert.shtml. Last accessed 25 February 2007.
- [25] Superpass Company, “5.25-5.9GHz 8dBi Omni-directional Antenna,” <http://www.superpass.com/SPDJ6O.html>. Last accessed 25 February 2007.
- [26] Hyperlink Technologies, “5.8GHz 8dBi ISM / UNII Band Omnidirectional Wireless LAN Antenna HyperGain HG5808U,” <http://www.hyperlinktech.com/web/hg5808u.php>. Last accessed 25 February 2007.
- [27] TerraWave Solutions, “TerraWave Solutions 5.7-5.85 GHz 10dBi Fiberglass Omnidirectional Antenna with N-Style Jack Connector,” <http://www.terrawaveonline.com/Dynamic/pdf/T58100O10006.pdf>. Last accessed 25 February 2007.
- [28] Hyperlink Technologies, “5.8GHz ISM / UNII Band 12dBi Professional Omnidirectional Wireless LAN Antenna HyperGain HG5812U-PRO,” http://www.hyperlinktech.com/web/hg5812u_pro.php. Last accessed 25 February 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Mr. Jim Ehlert
COASTS Program Manager
Naval Postgraduate School
Monterey, California
4. Mr. Edward L. Fisher
Lecturer of Information Sciences
Naval Postgraduate School
Monterey, California
5. Lieutenant Amy Bleidorn
COASTS Student Lead
Naval Postgraduate School
Monterey, California
6. Mr. Steve Iatrou
Student Advisor
Naval Postgraduate School
Monterey, California
7. Lieutenant Colonel Karl Pfeiffer
Program Officer
Naval Postgraduate School
Monterey, California
8. Mr. Peter Purdue
Dean School of Operational and Information Sciences
Naval Postgraduate School
Monterey, California
9. Colonel Bill Tarantino
Associate Dean School of Operational and Information Sciences
Naval Postgraduate School
Monterey, California

10. Dr. Dan Boger
Chairman, Department of Information Sciences
Naval Postgraduate School
Monterey, California
11. Mr. Scott Howard
Network Systems Engineer
Fortress Technologies, Inc.
Oldsmar, Florida
12. Group Captain Wanchai Tosuwan
Director, Research & Development Promotion Division
Parkred, Nonthaburi
13. Group Captain Dr. Triroj Virojtriratana
DRDO COASTS Project Manager
Parkred, Nonthaburi
14. Colonel Thomas Lee Williams
Deputy Science Advisor
U.S. Pacific Command (USPACOM)
Camp Smith, Hawaii
15. Mr. Russ Holland, Chief of Staff
Joint Inter-Agency Task Force West (JIATF-W)
Camp Smith, Hawaii
16. Mr. Kurt Badescher
US Special Operations Command (USSOCOM)
Tampa, Florida
17. Mr. J. Christopher Griffin,
Westwood Computer Corporation
Marlton, New Jersey
18. Mr. Ralph L. Boyce, US Ambassador of Thailand
US Department of State (DoS)
Bangkok, Thailand
19. Lieutenant Colonel Mel Prell, USAF
Joint US Military Advisory Group Thailand (JUSMAGTHAI)
Bangkok, Thailand

20. Lieutenant General Krita Kritakara
Deputy Secretary
Thailand National Security Council (NSC)
Bangkok, Thailand
21. Group Captain Wanchai Tosuwan
Director, Research & Development Promotion Division
Parkred, Nonthaburi, Thailand
22. Group Captain Teerachat Krajomkeaw
Directorate of Operations
Royal Thailand Air Force (RTAF) Headquarters
Bangkok, Thailand
21. Mr. John Laine
Senior Contractor, JIATF-West
Interagency Intelligence Fusion Center (IIFC)
Chang Mai, Thailand
22. Mr. Craig Shultz
Lawrence Livermore Laboratories (LLNL)
Livermore, California
23. Mr. Robert Sandoval
Joint Intelligence Operations Command (JIOC)
San Antonio, Texas
24. John Taylor
President, Mercury Data Systems
Greensboro, North Carolina
25. Captain Phil Erdie, USMC
U.S. Marine Corp Systems Command (MARCORSYSCOM)
Quantico, Virginia
26. Mr. Thomas Latta
C4ISR & IO PM
Space and Naval Warfare Systems Command
2721 C4ISR SE&IM Division, SSC-SD
80 Dept, 86 CND/IO OT&E Branch, COMOPTEVFOR
DOT&E IA&I/IO OT&E Assessment Programs
27. RADM Nimmick, USCG
Maritime Intelligence Fusion Center (MIFC)
Alameda, California

28. Mr. Jim Alman
President, CyberDefense UAV Systems
St Petersburg, Florida
29. Mr. Dennis B. D'Annunzio
COO, Rotomotion, LLC
Charleston, South Carolina
30. Mr. Curtis White
Commander's Representative
AFRL/XPW – AFFB/CCT
USAF Force Protection Battle Lab
Lackland AFB, Texas
32. Mr. Mike Rathwell
Identix Corporation
Jersey City, New Jersey
33. Dr. Leonard Ferrari
Dean of Research
Naval Postgraduate School
Monterey, California
34. Dr. Pat Sankar
NPS Distinguished Fellow
Naval Postgraduate School
Monterey, California
35. Dr. Gurminder Singh
Director of the Center for the Study of Mobile Devices and Communications
Naval Postgraduate School
Monterey, California
37. Dr. Frank Shoup
Director of Research, Meyers Institute, GSEAS
Naval Postgraduate School
Monterey, California
38. CAPT Michael L. Jordan, USN
Commander, Riverine Group ONE
Naval Amphibious Base
Little Creek, Virginia